jamf

Tiefenverteidigung (Defense-in-Depth, DiD)

Schließen von Sicherheitslücken durch Integration und Schichtung von Lösungen

Cybersicherheit ist nicht wichtig.

Es ist **von entscheidender Bedeutung**, Ihr Unternehmen vor sich entwickelnden Bedrohungen und Angriffen auf Ihre Geräte, Benutzer*innen, Daten und Ressourcen zu schützen.

Informationssicherheit war früher nicht viel mehr als eine auf jedem Computer installierte Antivirenlösung und ein VPN-Client für die wenigen Mitarbeiter*innen, die außerhalb des Büros arbeiteten, wie z. B. reisende Vertriebsteams.

Aber die Zeiten haben sich geändert und damit auch die Art und Weise, wie wir mit der Cybersicherheit umgehen.

In diesem Whitepaper behandeln wir die:

- Entwicklung der Bedrohungslandschaft
- Wichtigkeit des Schutzes aller Gerätetypen und Betriebssysteme
- Schlüssel zur Sicherheit, die über den Schutz von Ressourcen hinausgehen
- Kritische Bedeutungen der Umsetzung einer Defense-in-Depth -Strategie
- Die Bedeutung eines integrierten Sicherheitsansatzes für Unternehmen

Sich entwickelnde Bedrohungslandschaft

Die Branche hat einen weiten Weg zurückgelegt, und die Fortschritte in der Mobiltechnologie signalisierten Nutzer*innen und Unternehmen, dass sich die Art und Weise, wie die Arbeit erledigt wird, ändern würde. Diese Entwicklung ist noch nicht zu Ende. Auch die Bedrohungsakteur*innen änderten ihre Taktik und passten sich den Veränderungen durch die Weiterentwicklung von Bedrohungen und Angriffen an. Dadurch werden sie weitaus raffinierter - was bedeutet, dass sie für Endbenutzer*innen schwerer zu erkennen und für Sicherheitsexpert*innen viel schwieriger zu bekämpfen sind.

Einfach ausgedrückt: Bedrohungen kommen heute aus allen Richtungen. Sie sind für alle Gerätetypen und Betriebssysteme geeignet und können über eine beliebige Netzwerkverbindung bereitgestellt werden.

Warum, fragen Sie? Weil die Perimeter-basierte „Einzellösungsstrategie“, die einst relativ erfolgreich war, um die Sicherheit von Daten und Endpoints zu gewährleisten, unwirksam geworden ist. Die Netzgrenze wurde effektiv durch die:

- Umstellung auf Cloudbasierte Dienste und Apps
- Den Übergang zu entfernten/hybriden Arbeitsumgebungen
- Die Einbeziehung von privaten Geräten für die Arbeit
- Die Verwendung von nicht vertrauenswürdigen Netzwerkverbindungen für die Kommunikation
- Die Abhängigkeit von gemeinsamen Tools für die Zusammenarbeit

Jeder dieser Punkte hat den Nutzer*innen zweifellos die Möglichkeit eröffnet, von jedem Ort aus, zu jeder Zeit, auf jedem Gerät und über jede Netzverbindung zu arbeiten, unabhängig vom physischen Standort oder den Präferenzen in Bezug auf Architektur oder Software. Sie haben auch die potenziellen Angriffsvektoren vergrößert, indem sie einen größeren Teil der Angriffsfläche eines Geräts freigelegt haben.

Im Folgenden werden einige der verschiedenen Arten vorgestellt, in denen sich die Bedrohungslandschaft entwickelt hat, um der Zunahme mobiler Technologien und verteilter Arbeitskräfte Rechnung zu tragen.

APTs, konvergierte Bedrohungen und zunehmende Komplexität der Angriffe

Die Bedrohungslandschaft hat sich weiterentwickelt. Jeder Sicherheitsexperte/jede Sicherheitsexpertin, der/die etwas auf sich hält, weiß, dass diese Aussage wahr ist. Aber wie genau sich die Landschaft verändert hat, das ist das Ziel dieses Abschnitts. Ein Schadprogramm ist ein Schadprogramm - egal, ob es in einem Wrapper enthalten ist, der sich als App ausgibt, oder ob es über eine kompromittierte Website ausgeführt wird - das Ergebnis ist und war immer dasselbe: Ihr Gerät zu infizieren und es dazu zu bringen, Aufgaben auszuführen, die der Angreifer/die Angreiferin ausführen möchte.

Was wir sehen, ist eine Abkehr von der Formel 1 + 1 = 2, auf die man sich so viele Jahre lang verlassen hat. Die Angriffe sind immer komplexer geworden und werden häufig mit anderen Bedrohungen kombiniert oder auf andere Weise eingesetzt, z. B. indem ein vertrauenswürdiger Partner des Ziels kompromittiert wird, was wiederum einen Backdoor-Zugang zu den Ressourcen des Ziels ermöglicht. Einige dieser raffinierten Angriffe, die nur ein bis drei Jahre zurückliegen, sind Beispiele:

- Zwei Angriffe in ebenso vielen Jahren betrafen mehr als **100 Millionen** Kund*innen, indem ihre personenbezogenen Daten kompromittiert wurden.
- 2023 verdreifachten sich die Angriffe auf die Lieferkette mit **2,1** Milliarden Downloadsmit bekannten Sicherheitslücken (wenn korrigierte Versionen verfügbar waren).
- Casino and Hotel erlebte einen Ransomware-Angriff, der auf eine Social-Engineering-Kampagne zurückging, den Betrieb beeinträchtigte, Kundendaten kompromittierte und zu finanziellen Verlusten führte.
- Die Daten von **5,4 Millionen Nutzer*innen**sowie die öffentlichen und privaten Daten vonweiteren **400 Millionen Nutzer*innen wurden im Dark Web verkauft**, nachdem die API einer Social-Media-Plattform kompromittiert worden war.
- Personen mit hohem Risiko werden ständig von Nationalstaaten ins Visier genommen, die Pegasus-Spionageprogramme einsetzen, um die Privatsphäre durch die unerlaubte Überwachung von Mobilgeräten in persönlichem Besitz zu beeinträchtigen.

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, die die Reichweite von Angriffen vergrößern, noch verschärft, was zu größeren Auswirkungen führt:

- Beharrlichkeit erreichen
- Rechteausweitung
- Seitliche Bewegungen
- Einsatz von Malware
- Exfiltration von Daten

Wir sehen dies bei Unternehmen aller Branchen, da 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.

Dies war der Fall, als die größte Pipeline für raffinierte Ölprodukte in den USA, die 3 Millionen Barrel Kraftstoff pro Tag transportieren kann, nach einem Ransomware-Angriff im Jahr 2021 für fünf Tage stillgelegt werden musste. Die Auswirkungen auf diese kritische Infrastruktur? Am meisten wurde über das Lösegeld in Höhe von 5 Millionen Dollar berichtet, das an die Bedrohungsakteur*innen gezahlt wurde, um wieder Zugang zu den verschlüsselten Systemen und Daten zu erhalten. In den folgenden Jahren haben sich infolge des Anschlags mehrere Änderungen ergeben. Die aggressivere Vorgehensweise des Justizministeriums bei der Zerschlagung von Infrastrukturen und Kriminellen, die hinter Ransomware-Angriffen stecken, ist eine davon. Doch auch die Bedrohungsakteur*innen 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/eine Betrügerin, der sich als Mitarbeiter*in eines Unternehmens ausgab, oder eine E-Mail von einem großzügigen, aber besorgten Prinzen, der Ihr Bankkonto dringend benötigte, um seine Millionen zu behalten.

Oh, wie sich die Zeiten geändert haben.

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. Speer-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*innen, 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 Technik zur Aufrechterhaltung der Sicherheit nach einem Exploit, die einen funktionierenden Flugzeugmodus zeigt. Ein Blick unter die Oberfläche zeigt jedoch, dass Bedrohungsakteur*innen nach einem erfolgreichen Geräteangriff Systemdateien bearbeitet haben, die die Benutzeroberfläche so steuern, dass Flugzeugmodus-Symbole angezeigt werden und gleichzeitig der Internetzugang für alle Anwendungen außer der App des Angreifers/der Angreiferin deaktiviert wird. Auf diese Weise kann der Angreifer/die Angreiferin den Zugriff auf das Gerät aufrechterhalten (Persistenz), selbst wenn der Benutzer/die Benutzerin glaubt, dass er das Gerät erfolgreich offline gestellt hat.

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 genauso angreifbar bleibt, weil Bedrohungsakteur*innen 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 Bedrohungsakteur*innen weiterhin Zugriff auf und Kontrolle über ihre mobilen Geräte haben.

Nationalstaatliche/gezielte Angriffe

Im digitalen Zeitalter sind Gefühle der Paranoia in Bezug auf jede Handlung, jedes gesprochene Wort und jede beantwortete Nachricht - ob in der Öffentlichkeit, im Büro oder in der Privatsphäre des eigenen Zuhauses - gerechtfertigt, wenn man bedenkt, wie sehr die Technologie alle Bereiche unserer Existenz durchdrungen hat.

Selbst wenn Sie, wie Christopher Walken, keinen Computer oder kein Smartphone besitzen, besteht dennoch die Gefahr, dass Ihre Privatsphäre durch die Nutzung von Mobilgeräten in Ihrer Umgebung beeinträchtigt wird.

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 wichtigsten Zielsektoren weltweit sind:

Bildung **16%**

Regierung **12%**

Think Tanks/NGOs und IT mit jeweils **11%** gleichauf

9 von 10 Unternehmen glauben, dass sievon staatlich unterstützten Bedrohungsakteur*innen angegriffen wurden

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

5 APTs wurden (bisher) dabei beobachtet, wie sie KI als Waffe einsetzen, 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 Bedrohungsakteur*innen 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*innen vermischt. Und das ist noch nicht alles: Nationalstaaten nutzen die gesammelten Daten, um weitere Opfer wie Journalist*innen, Politiker*innen 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
- Schützen Sie Ihre Daten mit Antimalware-Lösungen
- Sicherer Tunnel-Fernzugriff über ein VPN

Veraltete Lösungen, die für den Schutz statischer Endpoints 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 „eingeschränkten Endpoints“ auf Unternehmensressourcen zuzugreifen. Die Möglichkeit, dass sie Risiken in Ihr Netzwerk einbringen, ist sehr real - und schlimmer noch: Die Administrator*innen werden sich dessen erst bewusst, nachdem ein Vorfall eingetreten ist.

Was ist dann die beste Vorgehensweise?

IT- und Sicherheitsteams sind in der Lage, Endpoints 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 Endpoints in ihrer Infrastruktur.

macOS im Unternehmen

Berücksichtigen Sie Ihre Unternehmensumgebung. Wahrscheinlich verwalten Sie Windows-basierte Geräte für Ihre Arbeit, aber wie stehen Sie zu macOS Computern und Laptops? Laut einer kürzlich durchgeführten Umfrage unter kleinen und mittelständischen Unternehmen „verwenden **55 %** der Unternehmen selbst Mac Geräte oder billigen deren Einsatz im Unternehmen ausdrücklich“, und zwar unabhängig von der Branche.

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

Weltweit:	U.S.:
15,46%	**25.02%**

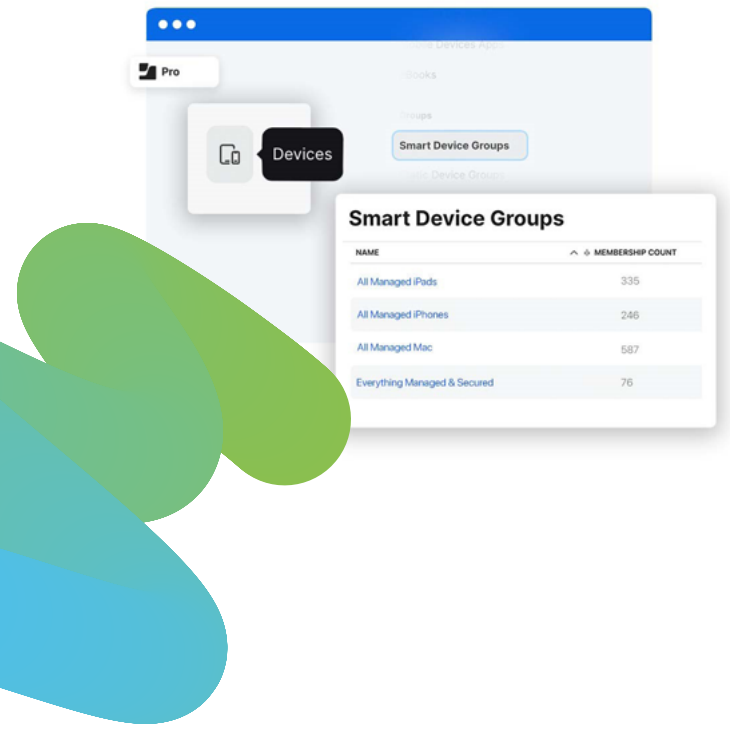
Allein in den USA beherrscht macOS ein Viertel des Marktes, wobei etwas mehr als die Hälfte davon in Unternehmen eingesetzt wird. Die bessere Frage wäre also: Wie sichern Sie macOS Endpoints, wenn (nicht wenn) sie in Ihrem Unternehmen eingesetzt werden? Denn ob es Ihnen gefällt oder nicht: macOS wird wahrscheinlich in gewissem Maße von Ihren Endbenutzer*innen verwendet, um arbeitsbezogene Aufgaben auszuführen. 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 ein Benutzer/eine Benutzerin 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 Nutzer*in im Jahr 2023 weltweit auf 3,6 ansteigen.

Das sind viermal mehr Angriffsvektoren pro Benutzer*in. 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 Endpoint-Sicherheitssoftware, 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 Bedrohungsakteur*innen 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 Compliance:** Das Fehlen einer richtlinienbasierten Durchsetzung führt dazu, dass Unternehmen haftbar gemacht werden können, wenn Geräte die Compliance 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 Bedrohungsakteur*innen.
- **Seitliche Bewegung:** Netzwerkbasierte Angriffe nutzen kompromittierte Anmeldeinformationen, um Angriffe auf die gesamte Infrastruktur auszuweiten und so das Ausmaß von Datenschutzverletzungen zu vergrößern.
- **Umgehung von Schutzmaßnahmen:** Falsch konfigurierte Sicherheits- und App-Einstellungen führen zu größeren Angriffsflächen und machen es Bedrohungen leichter, Nutzdaten auf Geräten ohne Schutzmaßnahmen auszuführen.
- **Ausweitung von Privilegien:** Schwachstellen in veralteter Software können ausgenutzt werden, sodass Bedrohungsakteur*innen in Geräte und damit auch in Ihr Netzwerk eindringen können.

Über den reinen Ressourcenschutz hinausgehen

Wenn es um die Schließung von Sicherheitslücken geht, gibt es eine natürliche Entwicklung im Denken der Sicherheitsexpert*innen, die sich verschiedene Möglichkeiten zur Risikominderung vorstellen. Die Verfeinerung von Patch-Management-Prozessen, damit Software und Betriebssysteme auf dem neuesten Stand und gegen bekannte Bedrohungen geschützt bleiben, ist ein gängiger Gedanke. Eine andere Möglichkeit wäre, die jüngsten Trends im Bereich der künstlichen Intelligenz (KI) zu nutzen und die Technologie des maschinellen Lernens (ML) in Ihr Sicherheitssystem zu integrieren, um schneller auf Vorfälle zu reagieren oder die Bedrohungssuche durch Automatisierung zu optimieren.

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*innen 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*innen 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.

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 Bedrohungsakteur*innen 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 Endpoints, die auf Unternehmensressourcen zugreifen, werden gleich behandelt - unabhängig davon:

- Gerätetyp
- Formfaktor
- Betriebssystem
- Apps und Dienste

Compliance

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 Administrator*innen, der sie warnt, wenn Endpoints aus den akzeptablen Parametern der Baseline ausscheren, und zeigt
an, dass sie möglicherweise nicht mehr konform sind.

Erbringung von Nachweisen für Prüfer*innen

Unabhängig davon, ob Ihr Unternehmen interne Prüfer*innen 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 Prüfer*innen, wenn es um den Nachweis der Konformität von Endpoints geht: „Wenn es nicht dokumentiert ist, ist es nicht passiert."

Der Schlüssel zur Verwaltung von Baselines und zum Sammeln von Beweisen für Audits liegt in Telemetriedaten. Sie bietet Administrator*innen einen Einblick in den Zustand der Endpoints 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.

> „Cybersicherheit ist viel mehr als eine Frage der IT“.
>
> — Stephane Nappo

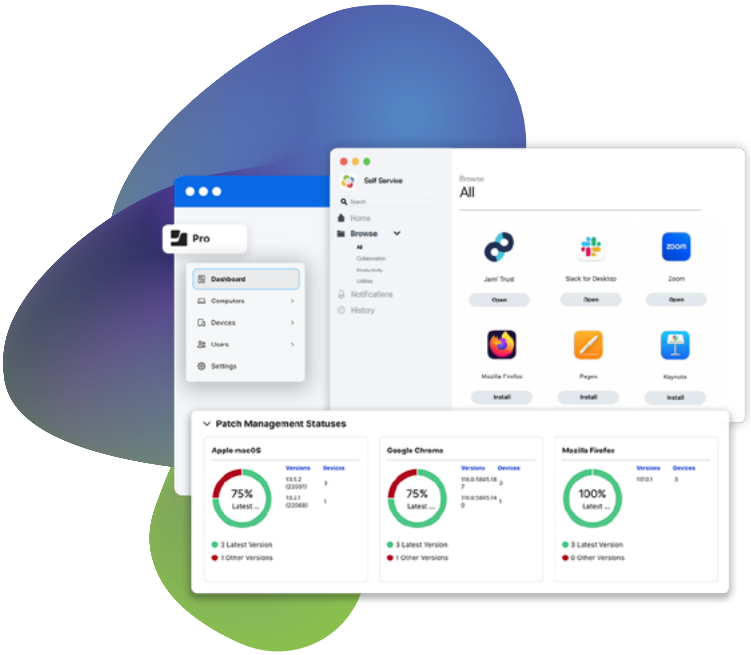
Der Begriff Konsolidierung bezieht sich hier auf die Zusammenführung von IT- und Sicherheitsexpert*innen zu einem einheitlichen Team. Dies ist eine Abkehr von der ungleichen Arbeitsweise der beiden Teams. Obwohl beide unter dem Oberbegriff Informationstechnologie zusammengefasst werden, haben Unternehmen 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 Anbieter*innen 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 Unternehmensadministrator*innen sicherstellen, dass Geräte und Benutzer*innen 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 Administrator*innen 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 Endpoints 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 Administrator*innen 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*innen 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*innen unerlässlich

sind Mitarbeiter*innen, 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*innen 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: 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*innen und/oder autorisierte Geräte den notwendigen Zugang zu geschützten Ressourcen auf der Grundlage zugewiesener Berechtigungen erhalten.
- **Endpoint-Sicherheit:** Softwarebasierte Technologien zur Risikominimierung und zum Schutz von Geräten und Benutzer*innen 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, Endpoint-Risikovektoren minimiert werden und Benutzer*innen 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 Netzwerkzugang (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 Administrator*innen 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/die Benutzerin 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*innen 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
- Administrator*innen 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 Administrator*innen von der Endpoint-Sicherheitssoftware 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.

Sichere Basislinien einrichten

Baselines, die sich auf die Cybersicherheit beziehen, beziehen sich auf den normalen Betrieb von Unternehmensendpoints. Der Aufbau einer Baseline erfordert mehr als nur die Messung der Leistung, sondern auch sichere Konfigurationen, Einstellungen, Endpoint-Sicherheitssoftware, 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 Administrator*innen besser feststellen, ob der Zustand der Endpoints innerhalb akzeptabler Grenzen liegt. Ist dies nicht der Fall, werden die Administrator*innen durch die Endpointprotokollierung 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 von Endpoints, 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.

Stoppen Sie netzwerkbasierte Bedrohungen

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.

Isolieren und Verschlüsseln von Verbindungen

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 Benutzer*innen 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 Endpoints und der Zugriffsanfragen

Anstatt Geräten implizit zu vertrauen, erfordern Null-Vertrauens-Modelle bei jeder Anfrage eine Überprüfung des Zustands von Endpoints und Anmeldeinformationen. Es vergleicht den aktuellen Gesundheitszustand des Endpoints 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 Administrator*innen 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*innen/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*innen 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 mobilen Apps sind eine führende Angriffsfläche. **±2 %** aller iOS und **±10 %** aller Android Mobilapps 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 Gesundheitszustand von Endpoints zu erkennen, die auf Ressourcen in Ihrem Unternehmen zugreifen, und um Risikofaktoren zu minimieren, bevor sie von Bedrohungsakteur*innen ausgenutzt werden können.

Nach Abschluss der Aufgabe scannt die Endpoint Security-Lösung 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

„Eine Unze Prävention ist mehr wert als ein Pfund Heilung“.

- Benjamin Franklin

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 des „Wann“ und nicht des „Ob“, ob Endpoints 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
- Administrator*innen 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 Reaktionsteams und Bedrohungsjäger*innen, 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 Endpoints 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*innen und Daten in Ihrer gesamten Infrastruktur ausweiten. Eine einzige, leistungsstarke Defense-in-Depth-Lösung, die Verwaltung, Identität und Sicherheit integriert.