jamf

Leitfaden für Käufer*innen: Mobilschutz

Stellen Sie sicher, dass Ihre Endpoints geschützt sind

Mobile Arbeitskräfte sind mit immer neuen Bedrohungen konfrontiert.

Die erfolgreicheBereitstellung von Mobilgeräten erfordert eine klare Übersicht sowie entschlossenes Handeln.

Mitarbeiter*innen arbeiten immer weniger am Schreibtisch oder im Büro, sondern auf Mobilgeräten. Die Verteidigung dieser verstreuten modernen Endpoints kann eine Herausforderung sein, zumal die Benutzer*innen neuen Bedrohungen ausgesetzt sind.

Cyberbedrohungen sehen es nicht nur auf unsere Computer ab. Die Gefahr für mobile Geräte ist real.

- **40 %** der beruflich genutzten Mobilgerätesind mit einer bekannten Schwachstelle behaftet.
- Bei Arbeiter*innen ist die Wahrscheinlichkeit, Opfer eines Phishing-Angriffs zu werden, auf einem Mobilgerät um **50 %** höher als auf einem Laptop.
- **1 %** der auf Mobilgeräten tätigen Arbeiter*innen sind von Malware betroffen, aber die fortgeschrittenen anhaltenden Bedrohungen (APTs) erlauben es Angreifenden, Benutzer*innen mit großer Präzision anzugreifen

Deshalb ist **Mobilschutz** entscheidend, wenn es darum geht, Ihre Mitarbeiter*innen, deren Mobilgeräte und Daten zu schützen. Zu einem robusten Programm für den Mobilschutz gehören:

- Die Verhinderung von Sicherheitsfehlkonfigurationen
- Das Blockieren von Angriffen
- Die Erkennung von Kompromissen durch robuste Forensik und Reaktion auf Vorfälle

Hauptmerkmale

Welche Sicherheitsfähigkeiten sollten Sie für einen Teil oder die Gesamtheit Ihrer Flotte in Erwägung ziehen?

Sichere Konfigurationsverwaltung

Abhärtung mobiler Geräte

- Einführung einer guten Sicherheitshygiene
- Durchführung von Compliance-Audits
- Überwachung auf Schwachstellen in der Konfiguration

Patch-Verwaltung

- Priorisieren Sie Patches mit detaillierten Berichten über Schwachstellen
- Entschärfen Sie Schwachstellen in OS und Apps

Beugen Sie Datenverlusten vor

- Kontrollieren Sie den Fluss von Unternehmensdaten zwischen Apps
- Schränken Sie den Zugang zu einer App basierend auf dem Sicherheitsstatus von Benutzer*innen und deren Geräten

Richtlinie zur akzeptablen Nutzung

- Schränken Sie die Webnutzung mit dynamischen kategoriebasierten Richtlinien ein
- Setzen Sie AUP nach Benutzer*in, Gruppe, Region oder globaler Konfiguration durch

Vorbeugung von Angriffen

Malwareund andere App-Risiken

- Blockieren Sie Malware
- Identifizieren Sie Schwachstellen und riskante Apps
- Verhindern Sie das Durchsickern wichtiger Daten während der App-Nutzung
- Überwachung der Nutzung alternativer Apps auf dem Marketplace

Adversary-in-the-Middle

- Identifizieren Sie abtrünnige Hotspots und Protokollangriffe
- Entschärfen Sie Adversary-in-the-Middle-Angriffe mit verschlüsselten Tunneln

Web-Bedrohungen

- Verhindern Sie Phishing-Versuche, einschließlich Zero-Day-Angriffen
- Blockieren Sie bösartigen Netzwerkverkehr, einschließlich C2 und Datenexfiltration
- Neutralisieren Sie das Risiko von Kryptojacking, Spam und anderen webbasierten Bedrohungen

Sicherer Zugriff

Schützen Sie Daten bei der Übermittlung

- Einrichtung verschlüsselter Tunnel zu wichtigen geschäftlichen Anwendungen und Daten

Audit der Nutzung kritischer Apps

- Erhalten Sie eine Berichterstattung über alle Apps, auf die mobile Arbeiter*innen zugreifen

Setzen Sie Richtlinien für den Zugang in Echtzeit durch

- Erstellen Sie Richtlinien für den Zugang, die Benutzer*innen und die Haltung der Geräte einbeziehen.

Erkennung von und Reaktion auf Bedrohungen

Reichhaltige Telemetrie sammeln

- Sammeln detaillierter Protokolle für die Offline-Analyse

Erkennung von Anomalien

- Aktivieren Sie die Bedrohungssuche und suchen Sie nach Anomalien, die auf bösartige Aktivitäten hinweisen.
- Binden Sie Indicators of Compromise sowie neue Erkenntnisse in die Threat Intelligence ein, um künftige Erkennungen zu optimieren

Bedrohungsbehebung

- Verweigern Sie den Zugang zu kritischen Apps und Workloads, wenn eine Gefährdung erkannt wird
- Entfernen Sie Malware und versetzen Benutzer*innen in einen produktiven Zustand zurück.

Erzielen Sie Trusted Access-Ergebnisse mit Jamf

Jamf hilft Organisationen, ihre wertvollsten Güter zu schützen, indem es sicherstellt, dass nur autorisierte Benutzer*innen auf registrierten Geräten, die den Sicherheitsanforderungen der Organisation entsprechen, Zugang zu sensiblen Geschäftsanwendungen erhalten.

Wählen Sie Ihre mobilen Sicherheitsfähigkeiten mit Bedacht

Die Bedrohungslandschaft und unsere Arbeitsmethoden entwickeln sich ständig weiter. Angemessene Schutzmaßnahmen von gestern sind keine Garantie für die Sicherheit von heute. Im Folgenden finden Sie einige Überlegungen zur Auswahl Ihrer Sicherheitslösungen für Mobilgeräte.

Untersuchen Sie die Fähigkeiten der Lösung.

Es ist wichtig zu prüfen, über welche Fähigkeiten Ihre Lösung tatsächlich verfügt. Es reicht nicht aus, dass sie eine Funktion für "Mobilschutz" vorgibt. Ihre Lösung sollte die einzigartigen Bedrohungen für mobile Geräte berücksichtigen und nicht einfach nur Computer-Sicherheitskonzepte auf ein Mobilgerät anwenden.

Sicherheit erfordert Geräteverwaltung.

Eine einzige Sicherheitslösung kann nicht alle Ihre Anforderungen erfüllen, und auch eine Software allein reicht nicht aus. Die Geräteverwaltung ist auf den Schutz bezogen von entscheidender Bedeutung, denn was man nicht sehen kann, kann man auch nicht sichern. Ihre Verwaltungssoftware hilft Ihnen, die Geräte-Compliance aufrechtzuerhalten und potenzielle Probleme zu beheben.

Das Erlebnis Ihrer Benutzer*innen ist wichtig.

Mitarbeiter*innen nutzen Mobilgeräte, weil ihre Mobilität ihnen hilft, produktiv zu bleiben. Sicherheitsrichtlinien, die die Funktionalität von Geräten zu sehr einschränken, sind für Benutzer*innen nicht hilfreich, da sie möglicherweise nicht genehmigte Umgehungslösungen aufsuchen könnten.

Mobile Geräte haben sich zu unverzichtbaren Arbeitsmitteln entwickelt, auf die sich Benutzer*innen verlassen, um produktiv zu bleiben. Wenn Geräte von der Aktion einer Richtlinie betroffen sind, müssen unbedingt Workflows eingerichtet werden, damit der/die Benutzer*in so schnell wie möglich wieder arbeiten kann.

Nicht alle Geräte benötigen die gleichen Sicherheits-Tools. Berücksichtigen Sie das Bereitstellungsszenario und den Anwendungsfall, bevor Sie Tools und Richtlinienkonfigurationen anwenden. Zum Beispiel:

- Überlegen Sie, wie Ihre Mitarbeiter*innen ihre Geräte nutzen. Ihre Rollen beeinflussen ihre Risiken. Ein Beispiel: Standard-Mitarbeiter*innen mit Zugang zu einigen sensiblen Daten und dem Internet müssen vor allgemeinen Bedrohungen geschützt werden. Ihre Geräte sollten die Compliance einhalten und vor Phishing und Malware geschützt werden. Die Filterung von Inhalten, die Abwehr von Bedrohungen und der Zero-Trust-Netzwerkzugriff tragen dazu bei, sie noch sicherer zu machen.
- Schreibtischlose Arbeiter*innen, wie im Einzelhandel, profitieren von der Filterung von Inhalten und der Sicherheit von Apps. Wenn ihr Gerät keinen Zugang zu einem Browser hat, ist die Gefahr des Phishings geringer.
- Führungskräfte und Arbeitsfunktionen mit Zugang zu kritischeren Daten sind oft das Ziel. Sie erfordern zusätzliche Schutzmaßnahmen und müssen häufig gesetzliche Anforderungen erfüllen.