DATENBLATT

proofpoint

PROOFPOINT MOBILE DEFENSE

SCHUTZ VOR APPS, DIE UNTERNEHMENSDATEN STEHLEN

Eine weitaus größere Gefahr als Mobilgeräte-Malware stellen für Unternehmen die Millionen allgemein verfügbaren Apps auf den Geräten der Mitarbeiter dar. Diese scheinbar harmlosen Apps, die unter die Rubrik „Riskware“ fallen, können zu Datenlecks, Diebstahl von Anmeldedaten sowie zur Exfiltration privater Informationen führen, die für gezielte raffinierte Angriffe auf bestimmte Mitarbeiter missbraucht werden.

„Im Jahr 2017 werden 75 % aller Sicherheitsverletzungen auf Mobilgeräten durch Apps und nicht durch gezielte technische Angriffe auf das Betriebssystem erfolgen.“

Gartner

Mitarbeiter gewähren diesen Riskware-Apps beiläufig umfangreiche Berechtigungen und sind sich dabei nicht bewusst, dass private Informationen sowie Unternehmensdaten möglicherweise an Remote-Server und Werbenetzwerke auf der ganzen Welt gesendet werden. Von dort können sie von Cyberkriminellen sowie gegnerischen Regierungen missbraucht werden, die Zugang zu Unternehmensnetzwerken suchen.

APP-BEDROHUNGSDATEN UND SCHUTZ FÜR DAS UNTERNEHMEN

Mobile Defense bietet Unternehmen umfassende Sicherheitsfunktionen sowie den Überblick, den sie zum Schutz vor böswilligen iOS- sowie Android-Apps benötigen, die ihre Daten gefährden und häufig zu hochentwickelten persistenten Bedrohungen (APTs), Spearphishing-Angriffen auf Mitarbeiter sowie Kompromittierungen von Unternehmensdaten führen.

Der Mobile Defense-Dienst arbeitet mit Lösungen für Mobile Device Management (MDM), Enterprise Mobility Management (EMM) und Mobile Security Management (MSM) zusammen, um App-Bedrohungen dynamisch zu erkennen sowie abzuwehren.

Mobile Defense basiert auf dem Proofpoint-Modul zur App-Analyse. Das Proofpoint-Team aus Analysten, Kryptographen und Cybercrime-Spezialisten hat bereits mehr als 2 Millionen kostenlose wie kostenpflichtige iOS- und Android-Apps von über 500.000 Herstellern analysiert. Zur Bestimmung des App-Risikos werden die einzelnen Apps auf mehr als 1.000 potenziell böswillige und für den Datenschutz relevante Verhaltensweisen überprüft.

STEUERUNGSFUNKTIONEN FÜR UNTERNEHMEN

- Verwaltungskonsole mit einer Dashboard-Übersicht des App-Risikos für das gesamte Unternehmen
- Möglichkeit zum Festlegen neuer Schwellenwerte für riskantes App-Verhalten und Beschränken bestimmter Verhaltensweisen
- Möglichkeit, bestimmte Apps auf die White- bzw. Blacklist zu setzen
- Benutzer und Administratoren erhalten Warnmeldungen, wenn Apps bestimmte Risikoschwellenwerte überschreiten
- Isolierung von Geräten oder Blockierung des Zugriffs auf Unternehmensdienste und -daten, bis riskante Apps entfernt wurden

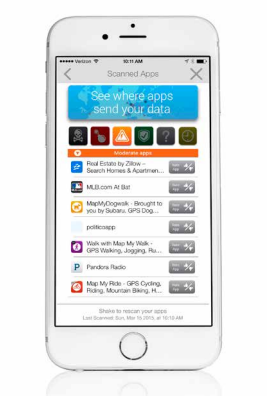
Die problemlos konfigurierbare Verwaltungskonsole von Mobile Defense umfasst ein Dashboard, auf dem Sie den Gesamtstatus der App-Sicherheit in Ihrer mobilen Umgebung ablesen können.

Sie erfahren durch den optionalen persönlichen Mobile Defense-Client, ob Sie gefährliche Apps heruntergeladen haben.

DER MOBILE DEFENSE-CLIENT

Mobile Defense umfasst eine optionale, mit führenden MDM- und EMM-Plattformen kompatible Mobilgeräte-Client-App, die Mitarbeiter in BYOD-Unternehmensumgebungen über das potenzielle Risiko der auf ihren Geräten installierten Apps informiert.

- Benutzer sehen auf einen Blick, ob eine App gefährlich oder sicher ist
- Sie bekommen Informationen darüber, wohin die App Daten sendet
- Auf das Gerät geladene Apps werden innerhalb von Minuten überprüft
- Anzeige einer Warnmeldung bei riskanten oder gefährlichen Apps mit der Aufforderung, diese App zu löschen



Mobile Defense zeigt Ihnen, an welchem Ort auf der Welt die App Ihre persönlichen Daten sendet.

AUTOMATISIERTER WORKFLOW

Mit Mobile Defense werden Ihre Workflows automatisiert:

- Mobile Defense identifiziert eine gefährliche App auf dem Gerät eines Mitarbeiters.
- Der Mitarbeiter erhält eine Warnmeldung mit dem Hinweis, dass eine gefährliche App vom Gerät entfernt werden muss.
- Wenn der Mitarbeiter die gefährliche App nicht rechtzeitig entfernt, wird das Gerät von Mobile Defense isoliert.
- Sobald die App entfernt wurde, wird der Zugang zu den Unternehmens-diensten wiederhergestellt.

Sie erfahren, welche Apps gefährlich sind und was im Hintergrund vorgeht.

PRIVATSPHÄRE DER MITARBEITER

Mobile Defense bietet mehrere Kontrollstufen, mit denen sichergestellt wird, dass das Unternehmen eine Vielzahl von Datenschutzbestimmungen und -gesetzen einhält. Folgende Stufen werden angeboten:

- Meldung aller Apps mit Verweis auf das Gerät eines bestimmten Benutzers
- Anonyme Meldung der Apps, ohne Verweis auf einen bestimmten Benutzer
- Kompletter Datenschutz ohne Informationen zur App – es wird nur gemeldet, dass sich eine gefährliche App auf einem Mitarbeitergerät befindet

VORTEILE VON MOBILE DEFENSE

Mobile Defense ist die marktführende Lösung für App-Bedrohungsdaten und App-Schutz. Durch die Kombination umfangreicher Analysedaten zu Mobilgeräte-Apps mit einem automatisierten Workflow erhalten Netzwerk- und Sicherheits-administratoren mit Mobile Defense genau die Informationen und den Überblick, um das Risikos durch Mobilgeräte-Apps in Unternehmen einzudämmen.

- Kontrolle über Apps, die Unternehmensdaten preisgeben
- Dynamische Bewertung von Bedrohungen mit Angaben dazu, wohin Daten gesendet werden
- Automatische Kontrollen für gefährliche Apps
- Sichere Implementierung eines BYOD-Programms für iOS- und Android-Geräte

INFORMATIONEN ZU PROOFPOINT

Proofpoint, Inc. (NASDAQ: PFPT) ist ein Cybersicherheitsunternehmen der nächsten Generation, das Unternehmen dabei unterstützt, die Arbeitsabläufe ihrer Mitarbeiter vor hochentwickelten Bedrohungen und Compliance-Risiken zu schützen. Dank Proofpoint können Cybersicherheitsexperten ihre Benutzer vor raffinierten und zielgerichteten Angriffen (per E-Mail, Mobilgeräte-Apps und Social Media) schützen, wichtige Informationen absichern und ihre Sicherheitsteams mit den notwendigen Bedrohungsdaten sowie Tools ausstatten, um bei Zwischenfällen schnell zu reagieren. Führende Unternehmen aller Größen, darunter mehr als 50 Prozent der Fortune 100, nutzen Proofpoint-Lösungen. Diese wurden für moderne IT-Umgebungen mit Mobilgeräten und Social Media konzipiert und nutzen die Möglichkeiten der Cloud sowie eine Big-Data-Analyseplattform zur Abwehr aktueller raffinierter Bedrohungen.