MOBILE THREAT DEFENSE

MOBILE BEDROHUNGEN

WBS IT-Service

Die mobilen Bedrohungen

Mobile Endgeräte weisen massive Sicherheitslücken auf: Was können wir tun, um uns trotzdem zu schützen?

Mobile Endgeräte dominieren unseren Business-Alltag. Denn wer hat es nicht – ein Handy, ein Tablet oder einen Laptop? Und spätestens seit dem verstärkten Einsatz von Homeoffice oder Mobile Working hat sich auch das damit einhergehende IT-Sicherheitsrisiko für die Unternehmen erhöht. Nur ist das nicht jedem Geschäftsführer auch gleichermaßen bewusst. Längst sind diese mobilen Plattformen aufgrund ihrer großen Verbreitung zum Ziel von Hackern und Datendieben geworden. **Mit Mobile Threat Defense lassen sich diese hohen Sicherheitsforderungen auch für mobile Endgeräte umsetzen**.

Was ist Mobile Threat Defense?

Mobile Threat Defense (kurz: MTD, deutsch: Mobiler Schutz vor Bedrohung) dient dem direkten Schutz Ihrer iOS- oder Android-Devices vor Cyberangriffen. Dabei nutzt die ausgewählte Software maschinelles Lernen und andere Technologien der künstlichen Intelligenz, um mögliche Bedrohungen zu erkennen und schnell darauf zu reagieren.
Der mobile Angriff geschieht unabhängig von der Art und Weise der Kompromittierung, z. B. durch Erlangen von Root-Zugriffen, Austricksen von Benutzern zur Installation bösartiger Profile oder kompromittierter Apps. Natürlich verwalten die meisten Unternehmen die mobilen Endgeräte ihrer Mitarbeiter längst zentral über eine UEM-Lösung (Unified Endpoint Management). Aber heutzutage reicht es nicht mehr aus, nur im Fall einer aktiven Bedrohung zu handeln, die Unternehmen müssen auch präventiv durch Risikoreduktion reagieren.
Mobile Threat Defense erweitert genau diesen Schutz. Es bietet proaktiven Schutz und automatisierte Problembehebung auf vier Ebenen an: Geräteebene, Netzwerkebene, Anwendungsebene und vor Phishing-Attacken.

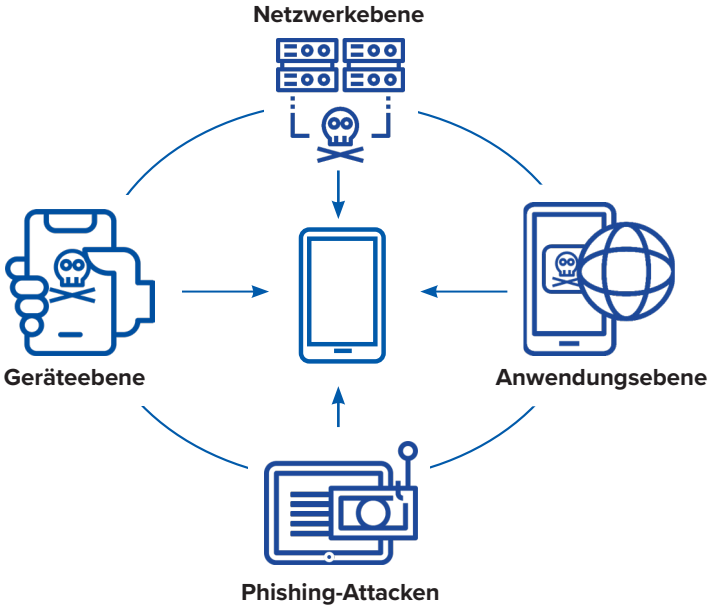

Abbildung 1: Ein Mobile Device ist auf vier Ebenen angreifbar.

Wussten Sie, dass ...

- **30 %** aller Malware *mobile* Malware ist?
- die Quote, mit der Nutzer eine mobile Phishing-URL anklicken, seit 2011 jedes Jahr im Durchschnitt um **85 %** gestiegen ist? [1]
- allein im März die Zahl der Cyberangriffe wegen Covid19 um **30 %** stieg? [2]
- im April 2020 Google z. B. jeden Tag **18 Mio.** Corona Scam* Mails blockierte? [3]
- bis zu **25 %** der Mitarbeiter bei Phishing-Tests auf gefälschte Links hereinfallen? [4]
- **80 %** aller Arbeitsaufgaben bis 2021 wahrscheinlich über Mobilgeräte erledigt werden?

* Scam-E-Mails: betrügerische E-Mails

Quellenangabe:
1 https://www.it-business.de/mobile-phishing-gefahr-fuer-nutzer-und-unternehmen-a-866101/
2 https://www.presseportal.de/pm/65324/4585470
3 https://www.bbc.com/news/technology-52319093
4 https://www.lookout.com/de/products/phishing-content-protection

WBS IT-Service GmbH • Friedrich-Ebert Str. 61 • 04109 Leipzig
+49 341 98271 0 mobile.solution@wbs-it.de www.wbs-it.de

1. Die Geräteebene

Hier prüft MTD das Betriebssystem selbst, ob alle **Zugriffe auf dem Gerät korrekt** sind, ob evtl. untypische Prozesse durchgeführt werden oder ob andere Vorgänge auf eine Infizierung mit Malware hindeuten. Des Weiteren wird das Gerät auf unbekannte Quellen, abnormalen Energieverbrauch, USB-Debugging und Authentizität kontrolliert.

Typische Angriffe auf der Geräteebene sind:
- „Kostenlose“ App-Downloads
- SMS-Nachrichten
- Vollständige Geräteübernahme
- Diebstahl verschlüsselter Inhalte

2. Die Netzwerkebene

Forschungen des US-Unternehmen Zimperium haben ergeben, dass 80 – 90 % aller mobilen Angriffe gegen ein Unternehmen mit einem Netzwerkangriff beginnen, zum Beispiel durch die Nutzung offener Wi-Fi-Netzwerke. MTD prüft hier, ob das mobile Gerät in dem eingewählten Netz möglicherweise im Hintergrund Scans oder Attacken ausgesetzt ist, die der Nutzer gar nicht bemerken würden. Mobile Security-Lösungen müssen also in der Lage sein, **netzwerkbasierten Bedrohungen sofort zu erkennen und diese zu bekämpfen**. Praktisch bedeutet das, die Erkennung muss auf dem Gerät selbst erfolgen und nicht in einer Cloud. Denn sobald der Angreifer das Netzwerk kontrolliert, wird der Zugang zu einer Cloud-basierten mobilen Antivirenlösung beendet und der Schutz ist nutzlos.

Angriffe auf der Netzwerkebene sind:
- Korrumpierte Access-Points
- Man-in-the-Middle-Attacken
- Abgehörte Kommunikationswege
- das Abgreifen von Nutzernamen, Passwörter und vertrauliche Firmendaten

3. Die Anwendungsebene (App-Ebene)

MTD kann die **auf dem Gerät installierten Apps überprüfen**, zum Beispiel ob diese ungewöhnliche Prozesse durchführen oder andere Prozesse des Gerätes nutzen, um sensible interne Daten nach außen zu übertragen.

Angriffe auf der App-Ebene sind:
- Installation von Apps aus Third-Party-App-Stores, die Malware enthalten
- Installation von Apps, die Malware enthalten
- eine App, erweiterte Zugriffsberechtigungen erfordert
- Angreifer führt Device-Exploit aus
- Eindringen in das Firmennetzwerk über kompromittierte Apps

„Mobile Security-Lösungen müssen längst ein obligatorischer Bestandteil Ihrer Unternehmensstrategie sein! Und genau das erfordert den Einsatz einer MTD-Software.“

Rico Müller
Service Account Management, WBS IT-Service GmbH

WBS IT-Service GmbH • Friedrich-Ebert Str. 61 • 04109 Leipzig
+49 341 98271 0 mobile.solution@wbs-it.de www.wbs-it.de

4. Phishing-Attacken

Über 60 % aller E-Mails werden auf einem mobilen Endgerät gelesen. Des Weiteren erfordert das mobile Arbeiten das Aufrufen von Links oder die Nutzung von Messenger-Diensten. Über all diese Formate können Sie Opfer von Phishing-Attacken werden. Umso wichtiger ist es, sich auf die Entwicklung und den Einsatz von Mobile Security Lösungen zu konzentrieren. Dabei muss **der Nutzer sensibilisiert und technologisch unterstützt** werden.

Mögliche Phishing-Attacken:

- Social Engineering
- Online-Nutzer auf Fake-Links leiten
- Downloads von Malware oder Exploit-Kits
- Credential-Phishing, Spear-Shishing, SMS-Phishing

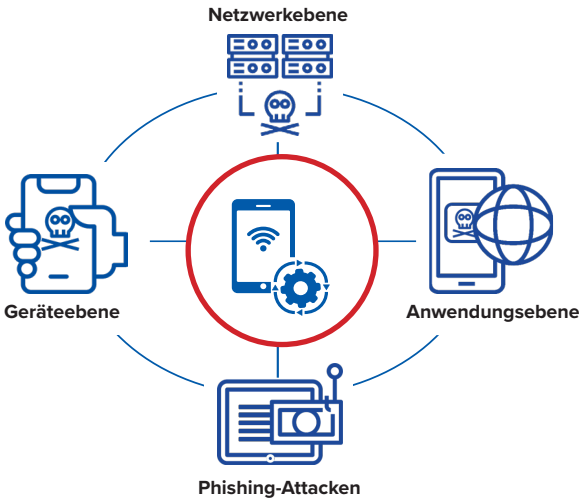

Abbildung 2: Mit einer MTD-Lösung ist das mobile Device auf allen vier Ebenen geschützt.

Zusätzlich: App-Reputation

Apps mit einer niedrigen Reputation nutzen mehr Zugriffsrechte, als sie für die eigentliche Anwendung benötigen. Sie sammeln Daten und Informationen, die sie nicht benötigen und bringen zusätzlich mögliche fehlerhafte Funktionen mit sich.

Wichtig: Achten Sie unbedingt darauf, dass Ihre App nur auf die Daten zugreift, die für die Verwendung der App dringend notwendig sind.

Die Vorteile einer MTD-Lösung

+ Das Betriebssystem Ihres mobilen Endgerätes ist längst nicht mehr gegen alle Cyberangriffe gesichert und **benötigt technische Unterstützung.**
+ MTD-Lösungen weisen **höchste Sicherheitsmaßnahmen** auf der Geräte-, Netzwerk- und Anwenderebene auf.
+ MTD-Lösungen schützen Ihr Gerät, auch wenn dieses **offline** ist.
+ MTD-Lösungen sind 100 % **DSGVO-konform.**
+ MTD-Lösungen stören den Workflow Ihrer Mitarbeiter:innen nicht und können **intuitiv** benutzt werden.
+ Die App wird direkt auf Ihrem Gerät installiert und **arbeitet im Hintergrund**. Sie ist mit dem Server des Anbieters verbunden und wird daher kontinuierlich mit den Updates zu aktuellen Bedrohungen versorgt.

WBS IT-Service GmbH • Friedrich-Ebert Str. 61 • 04109 Leipzig
+49 341 98271 0 mobile.solution@wbs-it.de www.wbs-it.de

„Die Mobilität hat sich mit der Pandemiesituation in diesem Jahr erhöht! Umso wichtiger ist es, dass Sie die mobilen Endgeräte Ihres Unternehmens und somit sensible interne Informationen sichern.“

Sebastian Schmutzler,
Head of Consulting Internet of Things, WBS IT-Service GmbH

Der Weg zur Ihrer Sicherheitslösung

Bevor Sie sich für eine MTD-Lösung entscheiden, stellen Sie sich folgende Fragen:

- Welche Daten befinden sich auf den Endgeräten?
- Für welche Workflows werden die Endgeräte eingesetzt?
- Wie hoch sind die Sicherheitsanforderungen an Ihre Daten?
- Wie hoch sind die Sicherheitsanforderungen an Ihre mobilen Endgeräte?
- Handelt es sich um BYOD- oder COPE-Devices?
- Ist eine Integration in das bestehende UEM-System möglich?
- Wie passt das MTD-Tool in die Security-Strategie meines Unternehmens?

Neben all diesen Fragen müssen Sie sich außerdem noch mit den anfallenden Kosten und dem möglichen Verwaltungsaufwand beschäftigen.

Das Forschungsunternehmen Gartner empfiehlt Unternehmen, MTD-Software schrittweise einzuführen und sie zuerst in sensiblen Bereichen einzusetzen.

Und genau hier können wir Sie unterstützen:
Wir beraten Sie herstellerunabhängig und zeigen, welche Lösung zu Ihren Vorstellungen und Wünschen des Unternehmens passt. Wir stehen Ihnen auch bei der Installation und Integration in die bestehende IT-Infrastruktur zur Seite.
Wir helfen darüber hinaus bei der Schulung ihrer Mitarbeiter und Mitarbeiterinnen sowie Administration und Überwachung.
Eine Auswahl an Herstellern, mit denen wir seit Jahren eng zusammenarbeiten:

Lookout

APPVISORY® by mediaTest digital

mobileiron The center of enterprise security

ZIMPERIUM® ADVANCED MOBILE SECURITY

10 | 112020 | ö

WBS IT-Service GmbH • Friedrich-Ebert Str. 61 • 04109 Leipzig
+49 341 98271 0
mobile.solution@wbs-it.de
www.wbs-it.de