



MOBILE ENDPOINT SECURITY

Strategische Beratung, Design,
Implementierung und Betrieb

Effektiver Schutz von Daten auf
mobilen Endgeräten

Der Trend, mobil zu arbeiten, nimmt stetig zu. Je mehr mobile Endgeräte am Future Workplace im Unternehmen genutzt werden, umso höher wird das Sicherheitsrisiko. Auf den Geräten werden eine Vielzahl von vertraulichen Daten gespeichert, wie beispielsweise Kontakte, E-Mails oder Geo-Lokationsdaten, auf die Angreifer abzielen. Studien belegen, dass die Wahrscheinlichkeit eines gezielten betrügerischen Angriffs auf Mitarbeiter (Phishing) auf mobilen Plattformen dreimal so hoch ist wie am Arbeitsplatzrechner.

Entwickler von Malware für Smartphones, allen voran mAPT-Programmierer (mobile Advanced Persistent Threat), haben es immer leichter, ihre Opfer zu täuschen. Wer glaubt, dass Phishing-Attacken immer noch hauptsächlich über E-Mails erfolgen, irrt. Gerade Apps werden immer häufiger zum Transportweg für Phishing.

Um dieses Einfallstor zu schließen und damit für sicheres mobiles Arbeiten zu sorgen, haben wir bei All for One Microsoft Office 365 und andere Microsoft-Lösungen mit der Post-Perimeter-Security-Architektur der Sicherheitsexperten von Lookout zu einer Lösung integriert.

Unser Partner Lookout ist Marktführer im Bereich Mobile Security (IDC) mit dem größten existierenden Daten-Set (170 Mio. User weltweit und 78 Mio. analysierte Apps). Lookout arbeitet eng mit Herstellern im mobilen Ökosystem wie Microsoft, Apple, Google Cloud etc. zusammen.

„DIE ABSICHERUNG MOBILER ENDGERÄTE IST FÜR UNS VON OBERSTER PRIORITÄT. WIR BETRACHTEN LOOKOUT ALS WESENTLICH, UM UNSERE UNTERNEHMENS DATEN VOR ANGRIFFEN ZU SCHÜTZEN UND SÄMTLICHE DATENSCHUTZVORSCHRIFTEN EINZUHALTEN.“



CHRISTIAN JÖSCH

Netzwerkadministrator,
SIMON HEGELE Gesellschaft für Logistik und Service mbH,
Karlsruhe

IHRE VORTEILE

☞ Sicherheit für Unternehmen, die mobile Endgeräte einsetzen, auf denen Unternehmensdaten sowie persönliche bzw. personenbezogene Daten bearbeitet werden.

☞ Erstellen von Sicherheitsrichtlinien für mobile Endgeräte macht mobiles Arbeiten sicher, ohne die Produktivität zu beeinträchtigen.

☞ Schutz von Informationen in der Cloud durch das Erkennen von vorhandenen Schwachstellen und Risiken auf mobilen Endgeräten.

☞ Identifizieren von mobilen Applikationen, die gegen die Compliance-Anforderungen verstoßen.

☞ Transparenz und Kontrolle über Datenlecks in Echtzeit.

☞ Gesamtpaket mit Partnerkomponenten: von der strategischen Beratung über Design und Implementierung bis hin zum Betrieb von der All for One Group als zentralem Ansprechpartner.

WARUM NEUE SICHERHEITSKONZEPTE?

Ob PC oder Mobile Device: Der Zugriff auf Anwendungen und -daten erfolgt über die Unternehmensinfrastruktur. Weil die Anzahl der mobilen Geräte und die Verfügbarkeit von Anwendungen stark gestiegen sind, müssen Schritte eingeleitet werden, um sensible Informationen zu schützen – die Ihres Unternehmens, Ihrer Assets, Ihrer Kunden und Partner. Dazu sind Investitionen in Mobile-Security-Lösungen und andere Sicherheitstechnologien unbedingt erforderlich.

Gefragt sind neue Sicherheitskonzepte, die über die Perimerebene oder Firewall hinaus gehen und Sicherheitslösungen wie Identity Management, Authentifizierungsverfahren sowie Cloud- und Endgeräte-Sicherheit einschließen. Denn Phishing- und andere Cyberattacken sind längst in der Lage, konventionelle Firewalls und Netzwerkgrenzen zu überwinden. Die Schutzmechanismen klassischer Mobile-Device-Management-Lösungen bieten bei der heutigen Bedrohungslage keinen ausreichenden Schutz mehr.

DAS **GESAMTPAKET** FÜR DEN SCHUTZ IHRER **MOBILEN ENDGERÄTE**

In sieben Schritten zum erfolgreichen Mobile-Security-Projekt

01

INITIALER WORKSHOP

Ein Projekt startet in der Regel mit einem eintägigen Workshop, in dem die Anforderungen definiert und Use Cases ausgearbeitet werden. Weitere Schritte sind die Planung und Dokumentation der Bereitstellung und die Definition der Meilensteine.

05

REVIEW DES POC

Review des POC auf Basis der Use Cases. Das Kunden-Feedback wird an dieser Stelle eingearbeitet. Hier erfolgt auch die Implementierung von Warnungen für die Endbenutzer, bevor Restriktionen auf den mobilen Endgeräten durchgesetzt werden.

02

AUFBAU EINES POLICY SETS

Gemeinsam mit Ihnen erarbeiten wir aus den definierten Use Cases und Anforderungen das „Security Policy Set“.

06

IMPLEMENTIERUNG

Die Implementierung umfasst den produktiven Rollout von Lookout auf alle Endgeräte sowie die Aktivierung. Zusätzlich können hier Sicherheitsmechanismen aus Microsoft Azure Active Directory integriert werden.

03

MDM CONNECT

Ist bereits ein Mobile-Device-Management-(MDM-)System implementiert, wird die Anbindung von Lookout geplant und umgesetzt. Lookout kann aber auch als eigene Lösung betrieben werden.

07

BETRIEB UND KONTINUIERLICHE OPTIMIERUNG

Wir empfehlen, das Policy Set kontinuierlich zu überprüfen, um den Sicherheitslevel permanent an neue Bedrohungsszenarien und Risiken anzupassen.

04

PROOF OF CONCEPT (POC)

Erstellung eines POC mit den vordefinierten Use Cases, um Funktionen sowie den Rollout zu testen. Wir empfehlen, dass die Anzahl der User eine repräsentative Größe aufweist.

IHR NUTZEN

☞ Schutz sensibler Unternehmensinformationen und -daten bei Zugriff von einem mobilen Endgerät aus.

☞ Erkennen von vorhandenen Schwachstellen und Risiken auf den Endgeräten, Apps und im Netzwerk, wie zum Beispiel manipulierte Betriebssysteme sowie Cyber-Attacken oder gezielte Phishing-Angriffe.

☞ Erhöhung der Daten- und Identitätssicherheit und damit verbunden die Unterstützung bei der Erfüllung der GDPR / DSGVO.

☞ Real-Time-Informationen zu aktuellen Bedrohungen und Risiken.

☞ Ausarbeitung eines Security Frameworks und Guidelines zur Umsetzung von Security und Compliance innerhalb Ihres Unternehmens.

DAS ALL FOR ONE PAKET FÜR IHRE **MOBILE ENDPOINT SECURITY**

DAUER

Insgesamt 5 Tage

- Initial Workshop: 1 Tag
 - Implementierung und Konfiguration: 3 Tage
 - Review: 1 Tag
-

REFERENTEN

1 Senior Consultant

ORT

In Ihrem Unternehmen oder in einer unserer Niederlassungen

LEISTUNGSBESCHREIBUNG

Workshop, Beratung, Implementierung und Konfiguration, Review und schriftliche Dokumentation

KOSTEN

zzgl. MwSt.

5.900 €

Gerne stehen wir Ihnen für ein
unverbindliches Gespräch zur Verfügung.

All for One Group AG

Rita-Maiburg-Str. 40
70794 Filderstadt

Willi Prosen
Head of Sales Microsoft

☎ +49 711 788 07 - 599

📠 +49 175 4817 671

✉ willi.prosen@all-for-one.com