ZIMPERIUM

Der CISO-Leitfaden zum Aktivieren des O365-Zugriffs auf mobilen Geräten – verwaltet oder BYO

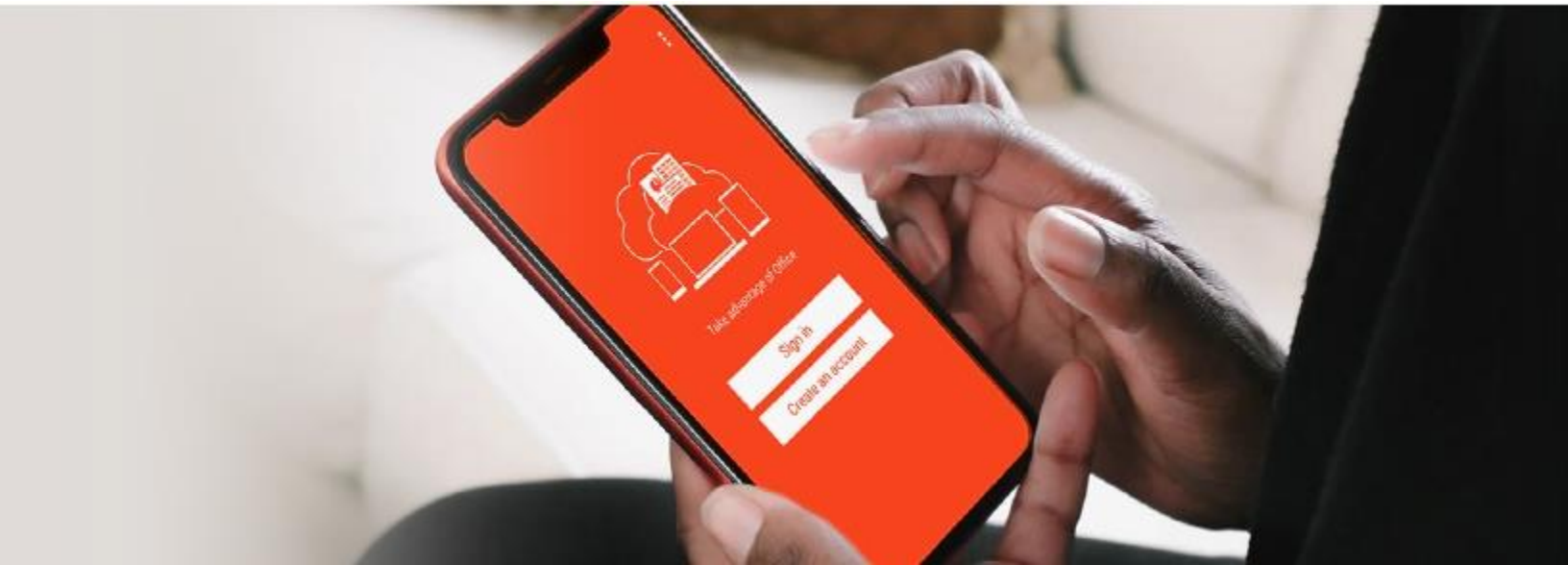
Einführung

Rund 84 % der Unternehmen haben Office 365 (O365) auf den mobilen Geräten ihrer Mitarbeiter aktiviert, doch mehr als 50 % haben keine Lösungen zur Abwehr mobiler Bedrohungen (MTD) implementiert, um sie vor Angriffen zu schützen. [1] Vor diesem Hintergrund haben wir Eric Green, der bei TikTok im Bereich Business Operations Protection arbeitet, gebeten, uns seine Ansichten darüber mitzuteilen, was Organisationen jetzt tun sollten, um sicherzustellen, dass der mobile Zugriff auf O365 sowohl nahtlos als auch sicher ist.

Z (Zimperium): Lassen Sie uns den Rahmen für dieses Thema abstecken, denn die effektive Sicherung des mobilen Zugriffs auf O365 war schon vor dem Ausbruch der Pandemie eine Herausforderung. Wie war das Umfeld und die Stimmung für Sie und Ihr Team, als der Lockdown im März 2020 begann?

Eric: Ich befand mich in meinem achten Monat als Global Head of Mobile & Mac Security bei HSBC. Niemand war auf die massiven operativen und sicherheitstechnischen Herausforderungen vorbereitet, denen wir uns bald gegenübersehen würden. Fast über Nacht stieg die Zahl der Mitarbeiter, die mobilen Zugriff auf O365 benötigten, massiv an. Das war problematisch, da **O365 auf Mobilgeräten Benutzern den gleichen Zugriff auf proprietäre und persönliche Unternehmensdaten gewährt wie vollständig gesicherte Desktops und Laptops.** Wir mussten sehr schnell handeln, um einen sicheren Zugang zu gewährleisten. Glücklicherweise hatten wir bereits eine solide MTD-Strategie entwickelt.

[1] Schnelle Umfragefragen, Dezember 2021 und Januar 2022 – home.pulse.qa –



Z: Wie haben Ihre Kollegen in anderen Unternehmen die Sicherheit des mobilen Zugriffs auf O365 gehandhabt?

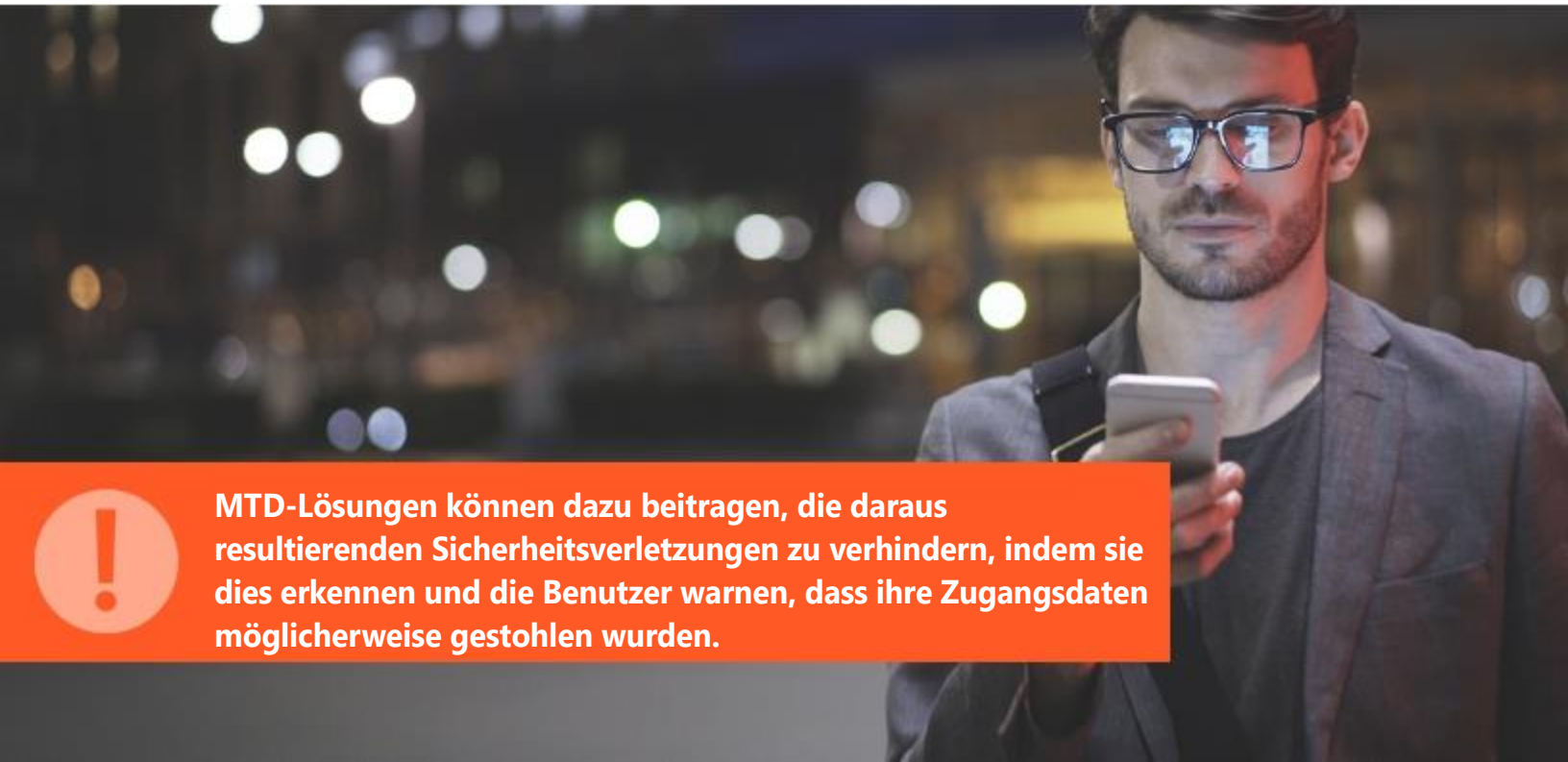
Eric: Die meisten Unternehmen wählten den traditionellen Ansatz und setzten UEM-Lösungen (einschließlich MDM und MAM) wie Microsoft Intune ein, um den Zugriff auf O365 und andere Ressourcen von Mobiltelefonen, Tablets und Laptops aus zu kontrollieren.

UEM UEM-Lösungen bieten die Transparenz, die zum Überwachen und Durchsetzen von Benutzerauthentifizierung, Datenzugriff und akzeptablen Nutzungsrichtlinien erforderlich ist. Wenn eine Risikostufe überschritten wird, können sie auch automatische Abhilfemaßnahmen ergreifen, wie z. B. das Deaktivieren einer O365-Anwendung, das Löschen des Geräts oder das Ausschalten des Geräts.

UEM-Lösungen können jedoch keine ausgeklügelten Phishing-, Malware-, geräte- und netzwerkbasierten Angriffe erkennen. Das Risiko für Unternehmen ist mit der rasanten Zunahme von Geräten im Besitz von Mitarbeitern exponentiell gestiegen. Durch die Pandemie wurde eine große und anfällige Angriffsfläche, die bereits extrem schwer zu überwachen und zu sichern war, dramatisch erweitert.

Z: Einige Organisationen haben vorgeschlagen, dass VPNs dabei helfen können, Office 365 auf Mobilgeräten zu sichern. Warum bieten sie keinen ausreichenden Schutz?

Eric: VPNs sind effektiv in Punkt-zu-Punkt-Situationen, in denen Sie den Datenverkehr zwischen mobilen Geräten und Ressourcen in den Räumlichkeiten verschlüsseln müssen. **Aber VPNs können mobile Bedrohungen weder erkennen noch darauf reagieren.** Sie eignen sich weniger für Szenarien, in denen man mit einem Browser auf Cloud-Dienste zugreift, vor allem, wenn der Datenverkehr vor dem Senden an die Cloud über ein Backhaul geleitet werden muss. Das treibt die Netzwerkkosten schnell in die Höhe und führt zu Leistungsengpässen für die Nutzer. VPN-Produkte sind zudem nicht narrensicher. Und wenn ein Angreifer die VPN-Anmeldedaten eines Mitarbeiters stiehlt, erhält er den gleichen Zugang zum Unternehmensnetzwerk. MTD-Lösungen können dazu beitragen, die daraus resultierenden Sicherheitsverletzungen zu verhindern, indem sie dies erkennen und die Benutzer warnen, dass ihre Zugangsdaten möglicherweise gestohlen wurden.



MTD-Lösungen können dazu beitragen, die daraus resultierenden Sicherheitsverletzungen zu verhindern, indem sie dies erkennen und die Benutzer warnen, dass ihre Zugangsdaten möglicherweise gestohlen wurden.

Z: Was ist mit Microsoft Defender für Endpoint? Wie gut werden mobile O365-Sicherheitsrisiken angegangen?

Eric: Es gibt Vor- und Nachteile. Ein Pluspunkt ist die integrierte Integration zwischen Microsoft-Produkten. So können Sie beispielsweise eine Dienst-zu-Dienst-Verbindung zwischen Defender und Intune herstellen, um Daten und Geräteprofile gemeinsam zu nutzen. So können Sie in Defender Risikostufen definieren, die in Intune bedingte Zugriffskontrollen auslösen.

Der Defender ist jedoch ein vergleichsweise neues Produkt, und die MTD-Funktionen sind primitiv. So liefert Defender beispielsweise nicht genügend Details über den Zustand eines mobilen Geräts, um genau zu bestimmen, ob es vertrauenswürdig, jailbroken oder kompromittiert ist. Ausgereifte MTD-Lösungen bieten umfassendere Funktionen zur Erkennung und automatischen Beseitigung von Bedrohungen auf Benutzer-, Geräte-, Anwendungs- und Netzwerkebene. Außerdem liefern sie die umfangreichen forensischen und telemetrischen Daten, die Analysten für die Ursachenanalyse und die Suche nach Bedrohungen benötigen.

Flexibilität und Zukunftssicherheit sind entscheidend. MTD-Lösungen sollten sich problemlos in Ihr SIEM, Ihren Identitätsanbieter und andere Sicherheitsinvestitionen integrieren lassen.

> „Defender liefert nicht genügend Details über den Zustand eines Mobilgeräts, um genau festzustellen, ob es vertrauenswürdig, jailbroken oder kompromittiert ist.“

Z: Wie geht MTD mit den Zero Trust-Initiativen um, die viele Unternehmen aufgrund von COVID beschleunigt haben?

Eric: Das Zero-Trust-Modell verlangt von Benutzern, Geräten, Netzwerken und Anwendungen, dass sie ihre Vertrauenswürdigkeit nachweisen, bevor sie Zugriff auf Ressourcen wie O365 gewähren. Die Herausforderung besteht darin, Zero Trust zu implementieren, ohne dass die Administratoren jede Interaktion überwachen müssen oder die Mitarbeiter gezwungen sind, für die Ausführung von Routineaufgaben sich ein Bein auszureißen.

MTD eignet sich gut für eine Zero-Trust-Umgebung, da es das mobile Gerät kontinuierlich auf Malware, Phishing-Exploits, betrügerische Zugangspunkte, von der Seite geladene Anwendungen und andere potenzielle Bedrohungen überwacht. Wenn ein Mitarbeiter nicht böswillig handelt oder sein mobiles Gerät versehentlich in Gefahr bringt, kann sein Zugang zu den Ressourcen ungehindert bleiben. Wenn MTD eine Bedrohung oder eine potenzielle Gefährdung feststellt, kann die Bedrohung sofort beseitigt werden, indem das Gerät in einen Zustand zurückversetzt wird, in dem es als vertrauenswürdig eingestuft ist.

Z: Wie beeinflussen die Unterschiede zwischen iOS und Android Ihren Ansatz zur Sicherung von O365 in einer hybriden Umgebung?

Eric: Die Tools und Workflows unterscheiden sich, aber die Ziele sind dieselben. Android Managed Work Profiles trennen Arbeitsanwendungen und -daten von persönlichen Anwendungen und Daten. Dies ermöglicht die Definition und Durchsetzung von Richtlinien zur Geräte-Compliance für Workspace-Apps, die konsistent angewendet werden, unabhängig davon, ob das Gerät eine Verbindung zu einem Cloud-basierten Dienst wie O365 oder zu einer Datenbank hinter der Unternehmensfirewall herstellt. Dies trägt dazu bei, die Risiken von BYO-Geräten zu verringern, ohne die Privatsphäre der Mitarbeiter zu verletzen. Apple holt mit seinem Profilmanager auf. Letztendlich werden die beiden Produkte gleichwertig sein.

Ansonsten spielen die Unterschiede zwischen den Betriebssystemen keine Rolle. Eine effektive MTD-Lösung sollte Bedrohungen erkennen und beseitigen, unabhängig davon, ob das Gerät mit iOS, Android oder ChromeOS (auf Chromebooks) betrieben wird.
Die Stärke des maschinellen Lernens liegt in der Erkennung von Bedrohungen auf der Grundlage ihrer granularen Merkmale und Prozessabläufe. Wichtig ist, dass diese Modelle und ihre Erkennungs- und Reaktionslogik lokal auf jedem mobilen Gerät eingesetzt werden (On-Device-Erkennung). Eine Kompromittierung kann innerhalb von Millisekunden erfolgen. Sie können sich die Latenzzeit, die mit Cloud-Suchvorgängen und Signaturabgleich einhergeht, nicht leisten.

„Eine effektive MTD-Lösung sollte Bedrohungen erkennen und beseitigen, unabhängig davon, ob auf dem Gerät iOS, Android oder ChromeOS (auf Chromebooks) ausgeführt wird.“

Z: Wie sieht es mit bewährten Verfahren für die Patch-Verwaltung aus? Was war Ihr Ansatz dabei?

Eric: Benutzer mögen es nicht, wenn man ihnen sagt, dass sie Patches installieren sollen, vor allem, wenn das mobile Gerät in ihrem Besitz ist. Viele halten sich nicht daran oder warten bis zur letzten Minute und sie kurz davor sind, den Zugriff auf Unternehmensressourcen zu verlieren. Einige mobile Geräte können nicht gepatcht werden, weil die Hardware veraltet ist. Sie müssen Prioritäten setzen. Betriebssystem-Updates sind von entscheidender Bedeutung, da sie häufig Sicherheitskorrekturen für kritische Schwachstellen bieten. Die Aktualisierung einer App ist in der Regel weniger dringlich, es sei denn, es handelt sich um eine autorisierte Arbeitsplatz-App wie Slack, die Mitarbeiter nutzen müssen, um produktiv zu sein.

Noch komplizierter wird es, wenn Sie eine Mischung aus iOS- und Android-Geräten haben. Apple-Benutzer sind in der Regel recht entgegenkommend. Sie sind es gewohnt, regelmäßig Patches und Updates zu installieren. Das Android-Ökosystem ist viel stärker fragmentiert. Hardware-Hersteller und Mobilfunkanbieter kontrollieren oft den Zeitpunkt und die Verfügbarkeit von Betriebssystem-Patches und -Releases. Letzten Endes spielen Sie ein Spiel, bei dem es um alles oder nichts geht. Sie müssen Patches auf der Grundlage des Risikoprofils Ihres Unternehmens und der Anforderungen des Anwendungsfalls nach Prioritäten ordnen. Es gibt keine perfekten Lösungen. Patching wird immer reaktiv sein.

Daher benötigen Sie eine Lösung, die Angreifer erkennen und daran hindern kann, Malware zu verbreiten und Schwachstellen auf jedem mobilen Gerät auszunutzen, unabhängig vom Eigentumsmodell oder Grad der Compliance.

Z: Wie würden Sie angesichts der aktuellen Bedrohungslandschaft Ihre Empfehlungen für CISOs zusammenfassen und abwägen, ob und wie man den mobilen Zugriff auf O365 sichern sollte?

Eric: Die Sicherung des mobilen Zugriffs auf O365 ist unerlässlich, aber ehrlich gesagt nur ein Teil eines viel größeren Puzzles. Arbeitnehmer werden auch in Zukunft über mobile Geräte auf alle Unternehmensressourcen zugreifen. Bedrohungsgruppen werden weiterhin neue Wege finden, um sie zu Fehlern zu verleiten und anfällige mobile Anwendungen und Betriebssysteme auszunutzen. Der Schlüssel liegt darin, die mobilen Bedrohungen zu identifizieren und zu priorisieren, die die größten Risiken für Ihr Unternehmen darstellen

Wenn Sie Intune verwenden, stellen Sie sicher, dass Ihre Richtlinien für die Geräteverwaltung diese Risiken berücksichtigen, ohne zu restriktiv zu sein. Schulen Sie Benutzer, um eine gute Cyber-Hygiene zu praktizieren. Vergewissern Sie sich, dass die Browser beim Zugriff auf Cloud-Dienste eine angemessene Verschlüsselung verwenden. Beschleunigen Sie den Übergang zu Zero Trust. Das deckt das grundlegende Blocken und Tackling ab.

Aber Sie müssen auch eine MTD-Lösung einsetzen, die nachweislich effektiv mobile Bedrohungen für Benutzer, Geräte, Netzwerke und Anwendungen erkennt und abwehrt.

Stellen Sie sicher, dass die von Ihnen gewählte Lösung gut mit Ihrer bestehenden Verwaltungs- und Sicherheitsinfrastruktur funktioniert und die Flexibilität bewahrt, die Sie benötigen, wenn sich Ihre Infrastruktur weiterentwickelt, um neue Sicherheitsherausforderungen zu meistern.