ZIMPERIUM.

Implementierung von Mobile BYOD in einer Zero-Trust-Umgebung

Das Perimeter-basierte Netzwerksicherheitsmodell, das Benutzer innerhalb eines Unternehmensnetzwerks als „vertrauenswürdig“ einstufte, bietet inzwischen nicht mehr das gleiche Maß an Sicherheit wie früher. Durch Cloud-Computing, Mobilität und Telearbeit ändert sich mittlerweile die Art und Weise, wie Menschen auf digitale Ressourcen zugreifen. Diese neuen Modelle haben zur Folge, dass Mitarbeiter zunehmend ihre eigenen Geräte verwenden möchten, wodurch Bring-Your-Own-Device-Richtlinien (BYOD) für die Sicherheit von noch größerer Bedeutung werden. Bei der Implementierung einer Zero-Trust-Architektur in einer BYOD-Umgebung sollte die Mobile Threat Defense (MTD) als Ergänzung zur Sicherheitstechnologie eingesetzt werden.

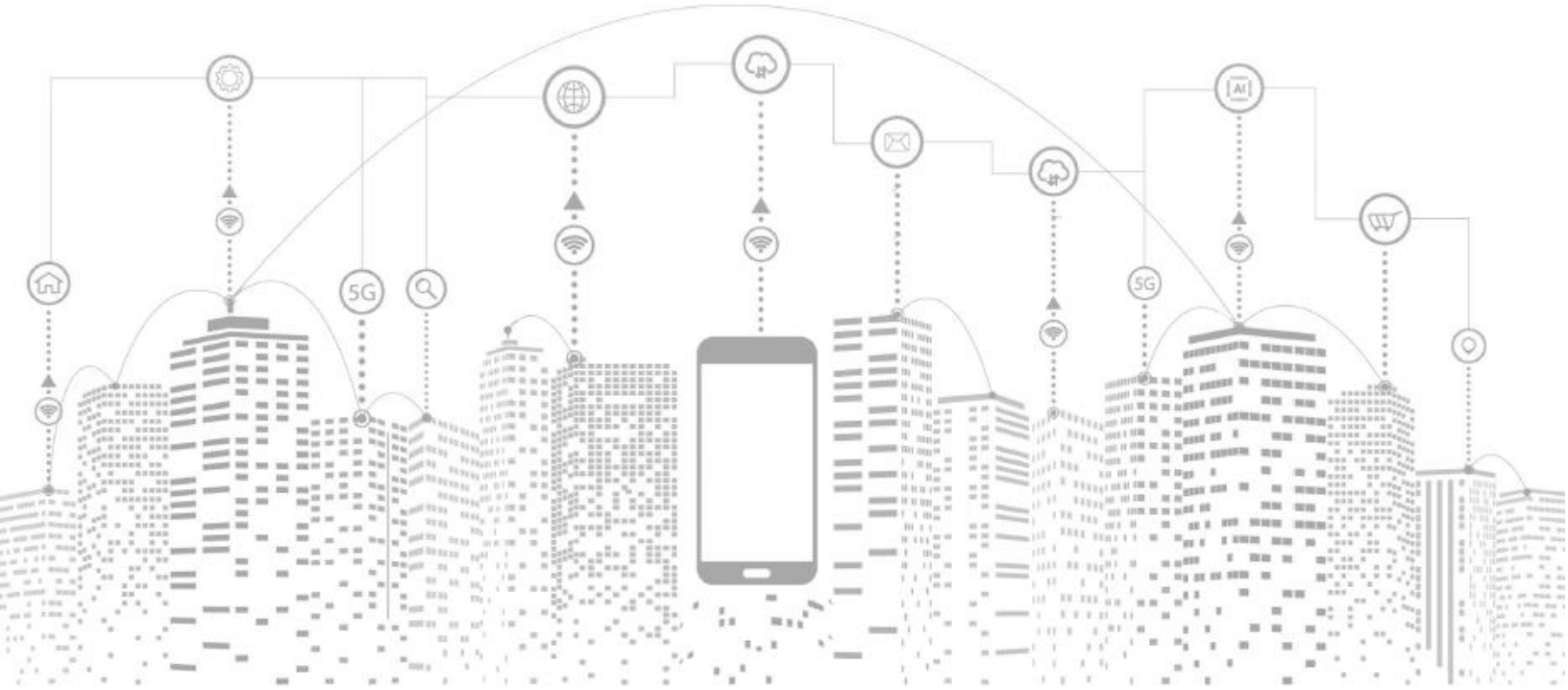
Warum Zero Trust?

Mit den neuen Technologien und Mitarbeitermodellen ändert sich die Art und Weise, wie Unternehmen dem Thema Sicherheit entsprechen müssen. So herrscht beispielsweise ein inhärentes Vertrauensverhältnis, wenn sich alle Benutzer und Geräte mit geschützten Netzwerken verbinden.

Die Menschen nutzen mittlerweile das öffentliche Internet – selbst innerhalb geschützter Netzwerke – um für berufliche Zwecke auf webbasierte Anwendungen zuzugreifen. Auch externe Geschäftspartner, wie Auftragnehmer, nutzen das öffentliche Internet, um ihren Verpflichtungen nachzukommen.

Bei einem Zero-Trust-Ansatz zur Sicherheit liegt der Schwerpunkt auf einem sicheren Ressourcenzugriff, welcher Folgendes umfasst:

- Integritätsnachweise für Geräte
- Schutzmaßnahmen auf Datenebene
- Identitäts- und Zugriffsmanagement
- Strategische Netzwerksegmentierung



Warum die Einhaltung von Zero Trust eine Herausforderung darstellt

Im Wesentlichen ist Zero Trust auf die folgenden sechs Hauptsäulen ausgerichtet:

Die Einhaltung von Zero Trust kann sich als eine ziemliche Herausforderung erweisen, denn innerhalb jeder Säule muss ein Unternehmen mehrere Aspekte absichern. Des Weiteren gibt es nur wenige Schritt-für-Schritt-Prozesse zur Einrichtung einer Zero-Trust-Architektur.

So müssen Unternehmen innerhalb der Säule „Geräte“ beispielsweise für kontinuierliche Sicherheit bei Workstations, mobilen Geräten (einschließlich Tablets und Smartphones), Internet-of-Things (IoT)-Geräten wie Druckern und Servern garantieren.

Unternehmen müssen in diesem Bereich die Gerätesicherheit verwalten, und zwar durch die Festlegung grundlegender Schutzmaßnahmen. Zudem brauchen sie einen Überblick über die künftige Sicherheit, was bedeutet, dass sie diese Richtlinien durchsetzen und eine ständige Risikobewertung der Geräte vornehmen müssen.

Bei der Überwachung zur Einhaltung von Richtlinien sollte dies wie folgt aussehen:

- **Traditionell:** Überblick darüber, ob ein Gerät die festgelegten Sicherheitsrichtlinien einhält
- **Fortgeschritten:** Fähigkeit, die Einhaltung der Richtlinien für die meisten Geräte durchzusetzen
- **Optimiert:** Überwachung und Validierung der Gerätesicherheit in Echtzeit

Viele Unternehmen haben in BYOD-Umgebungen Schwierigkeiten, sich einen Überblick darüber zu verschaffen, ob ein Gerät mit den festgelegten Sicherheitsrichtlinien konform ist. Vielleicht können sie nicht beeinflussen, welches Gerät von wem benutzt wird, oder haben Schwierigkeiten, die Datenschutzanforderungen zu erfüllen, wenn sie Technologien zur Verbesserung der Sichtbarkeit einsetzen.

Jedes Unternehmen sollte sich gegen diese Bedrohungen für mobile Geräte schützen

Eine ständige Geräteüberprüfung ist für eine erfolgreiche BYOD-Strategie zur Erfüllung der Zero Trust-Sicherheitsanforderungen unerlässlich. Unternehmen müssen bei der Ausarbeitung dieser Strategien und Initiativen verschiedene Bedrohungen berücksichtigen, die deren Ziele beeinträchtigen können. Da Mitarbeiter ständig mit ihren mobilen Geräten im Internet aktiv sind, sehen sie sich echten Bedrohungen ausgesetzt.

Phishing

Die verstärkte Ausrichtung auf Phishing-Angriffe durch Bedrohungsakteure ist nichts Neues. Einem Artikel von SC Media zufolge haben Phishing-Angriffe mit Ursprung in Russland zwischen dem 27. Februar und dem 1. März 2022 um das Achtfache zugenommen.

Unserem globalen Bericht über mobile Bedrohungen 2022 zufolge gaben 55 % der Befragten an, dass „Ausbeutung durch Phishing“ ihr größtes Risiko sei, wobei 61 % angaben, dass sie während der COVID-19-Pandemie einen Anstieg der Phishing-Angriffe erlebt hätten.

Obwohl die meisten Endbenutzer nicht wirklich die Absicht haben, Schaden anzurichten, fällt es angesichts der zunehmenden Raffinesse und der Flut von Aktivitäten schwer, die digitale Spreu vom Weizen zu trennen. Ein Ansatzpunkt sind herkömmliche signaturbasierte Antiviren- oder Phishing-Lösungen. Viele von ihnen sind jedoch reaktiv und werden der Vielzahl neuer Phishing-Seiten, die ständig erscheinen, nur bedingt gerecht.

Die Forscher von Zimperium haben allerdings einen besorgniserregenden Anstieg an Phishing-Websites festgestellt, die speziell auf mobile Geräte ausgerichtet sind. Bei der Analyse unserer sowie öffentlicher Daten, die über einen Zeitraum von zwei Jahren erhoben wurden, zeigte sich, dass die Zahl der mobilspezifischen Phishing-Websites um 50 % gestiegen ist. Darüber hinaus waren im Jahr 2021 bereits 75 % der analysierten Phishing-Websites speziell auf mobile Geräte ausgerichtet und lieferten Inhalte, die für das mobile Format ausgelegt waren.

Die Angreifer zielten beispielsweise mit den folgenden zwei Methoden auf mobile Geräte ab:

- **Adaptive Websites:** Adaptive Websites können je nach verwendetem Gerät unterschiedliche Inhalte laden und auf alternative Websites umleiten. Indem sie den Inhalt anhand des User-Agents eines mobilen Endgeräts anpassen, können Angreifer gezielt mobile Geräte angreifen.
- **Responsive Websites:** Da hier die Größe und Anordnung von Objekten an die Bildschirmgröße des Endgeräts angepasst wird, können Angreifer diese berechtigten Funktionen für ihre Angriffe auf mobile Geräte nutzen.

Bei mobilen Geräten kommt eine zusätzliche Ebene der Komplexität hinzu, die herkömmliche Antivirus- und Phishing-Ansätze für mobile Geräte unangemessen macht. Zum einen macht die Anbindung eines Geräts an eine Cloud, abgesehen von Bedenken hinsichtlich des Datenschutzes und der Latenzzeit, jeden Cloud-first-Ansatz sowohl aus technischer als auch aus betrieblicher Sicht unmöglich. Des Weiteren können mobile Geräte keine großen Signaturdateien herunterladen bzw. unterstützen, weshalb ein Rückgriff auf bekannte Datenbanken oder Bedrohungsinformationen weder angemessen noch durchführbar ist.

Somit sind die einzigen sinnvollen Alternativen für den Schutz mobiler Geräte solche, die unabhängig von der Cloud direkt auf dem Gerät eingesetzt werden können und sowohl bekannte als auch unbekannte Bedrohungen erkennen, ohne sie vorher gesehen haben zu müssen. Die z9-Erkennungs-Engine von Zimperium mit ihren Klassifikatoren für maschinelles Lernen (ML) bietet nicht nur Schutz vor Phishing, sondern auch vor Geräte-, Netzwerk- und Anwendungsbedrohungen.

Heruntergeladene Apps

Die Risiken, die von der Schatten-IT auf herkömmlichen Geräten ausgehen können, sind vielen Unternehmen bereits bekannt. Die Unfähigkeit, solche Anwendungen in Bestandsverzeichnisse aufzunehmen, führt jedoch zu mangelnder Transparenz.

Noch riskanter werden die auf mobile Geräte heruntergeladenen Apps. Da Mitarbeiter mobile Geräte sowohl privat als auch beruflich nutzen, können Unternehmen die Sicherheit der von ihnen verwendeten Anwendungen zur Verwaltung ihrer privaten Nutzung kaum noch kontrollieren.

Die Zusammenführung von mobilen bzw. Desktop-Apps in modernen Betriebssystemen ist eine Tendenz, welche es Bedrohungsakteuren erleichtert, mobile Geräte als Backdoor für Systeme und Netzwerke zu nutzen. Nach Angaben des Bedrohungsberichts von Zimperium meldeten 42 % der Unternehmen, dass nicht autorisierte Apps und Ressourcen auf Unternehmensdaten zugreifen.

Die MTD-Lösung von Zimperium dient ausschließlich der Vorbeugung, Erkennung und Bekämpfung von Bedrohungen für Geräte mit iOS, Android und Chrome OS. Eine Mobile-Device-Management-Lösung (MDM) kann zwar bei der Verwaltung und Durchsetzung von Richtlinien nützlich sein, doch MTD von Zimperium schirmt das Unternehmen durch die Unterteilung von sensiblen Informationen und Prozessen ab und verringert so die Angriffsfläche.

Malware in heruntergeladenen Apps

Die Angriffsfläche für mobile Geräte unterscheidet sich von der herkömmlichen Angriffsfläche, entsprechend einzigartig ist auch die mobile Malware. In manchen Fällen ist die App selbst die Malware, in anderen nutzen Angreifer Apps, um die Malware über eine Sicherheitslücke einzuschleusen.

Schädliche Apps

Die Analyse der mobilen Sicherheit von Zimperium deckte im Jahr 2021 insgesamt 2.034.217 neue Schadprogramme auf, die in freier Umgebung entdeckt wurden. Das sind durchschnittlich fast 36.000 neue Varianten von Malware pro Woche – über 5.000 pro Tag. So haben Angreifer in der Urlaubssaison 2021 gezielt Nutzer von Mobilgeräten mit SMS- und E-Mail-Links angesprochen, die für Rabatte warben, in der Hoffnung, die Nutzer würden diese zum Herunterladen einer schädlichen App nutzen.

Obwohl sich einige Varianten mobiler Malware wie herkömmliche Endpunktangriffe verhalten, sehen und handeln manche völlig anders. Einige können beispielsweise sein:

- Diebstahl von Anmeldedaten für die Zwei-Faktor-Authentisierung (2FA) über SMS- oder App-Benachrichtigungen.
- Durchführung von Overlay-Angriffen, bei denen ein Benutzer Anmeldedaten in eine sekundäre App eingibt, von der er glaubt, sie sei seriös.
- Überwachung anderer installierter Apps über Berechtigungen des Accessibility-Service. Nutzung der Standortverfolgung über GPS-Dienste.
- Verwendung der Standortverfolgung über GPS-Dienste.
- Aktivierung von Kameras oder Mikrofonen zur Aufzeichnung von Audio bzw. Video.
- Zugriff auf sensible Inhalte wie Fotos, Kontakte oder persönliche Daten.
- Erfassen und verfolgen von Sensordaten.

Gefährliche Apps

Da es sich bei mobilen Apps um eine neuere Technologie handelt, ist das Sicherheitsniveau im Entwicklungszyklus der Software möglicherweise nicht ganz so hoch, vor allem, weil Unternehmen versuchen, neue Erfahrungen möglichst schnell einzuführen.

Zimperium kam in der zweiten Hälfte des Jahres 2021 zu dem Ergebnis, dass etwa 81 % der weltweit mehr als 160 mobilen Finanz-Apps, die untersucht und analysiert wurden, möglicherweise sensible Daten preisgaben. Abgesehen von den Finanzanwendungen stellte Zimperium fest, dass 77 % der Android- und 46 % der iOS-Apps aus den Bereichen Gesundheit, Einzelhandel und Lifestyle mindestens einen anfälligen Verschlüsselungsalgorithmus verwenden oder möglicherweise verwenden könnten.

Anders ausgedrückt: Selbst wenn Endbenutzer seriöse Apps herunterladen, können diese ein Risiko für das Unternehmen darstellen. Unternehmen, deren Sicherheit bei der Entwicklung mobiler Apps noch in den Anfängen steht, sollten sich über den Schutz vor diesen Risiken Gedanken machen.

Netzwerkangriffe

Von überall aus zu arbeiten bedeutet, dass sich Mitarbeiter über unsichere WLAN-Netzwerke verbinden. Auch wenn dies nicht neu ist, sind Man-in-the-Middle (MitM)-Angriffe nach wie vor effizient. Laut einer von Zimperium durchgeführten Untersuchung waren 13 % der Geräte von MitM-Angriffen betroffen.

Ähnlich schwerwiegend ist die Tatsache, dass zuvor „geschützte“ WLANs durch „Evil-Twin“-Angriffe untergraben werden können, bei denen böswillige Akteure ein kostenloses WLAN vortäuschen, das ein Zugangsportal nutzt, z. B. in einem Hotel oder am Flughafen. Laut den Untersuchungen von Zimperium waren etwa 16 % der mobilen Geräte entweder mit einem bekannten böswilligen Netzwerkangriff, einer Manipulation des Datenverkehrs oder einem betrügerischen Zugangspunkt in Verbindung gebracht worden. Allerdings ist es wahrscheinlicher, dass Endbenutzer, die sich zuvor mit dem richtigen WLAN verbunden haben, darauf vertrauen, dass dieses sicher ist. Sobald sich der Benutzer jedoch über dieses gefälschte WLAN beim Unternehmensportal anmeldet, können die böswilligen Akteure dessen Anmeldedaten stehlen.

Durch Zimperium können Unternehmen bedingte Zugriffsanforderungen durchsetzen, wenn Mitarbeiter ihren Standort wechseln, da der „Gerätezustand“ ständig überwacht wird. Mit der MTD-Lösung von Zimperium hat das Unternehmen Einblick in die Gerätesicherheit und kann so den Zugriff über eine gefälschte WLAN-Verbindung gezielter verweigern.

Ladestationen

Bei der Betrachtung mobiler Risiken befürchten Unternehmen oft hauptsächlich Phishing. Wenn man sich jedoch ausschließlich mit Phishing befasst, werden andere Methoden zur Verbreitung von Malware außer Acht gelassen.

Die FCC hat kürzlich die Verbraucher gewarnt, dass öffentliche USB-Ladestationen, wie z. B. in Einkaufszentren und Flughäfen, von Cyberkriminellen ausgenutzt werden. Diese als „Juice Jacking“ bekannte Angriffsart kann über den USB-Anschluss oder ein von den Cyberkriminellen hinterlassenes Kabel ausgeführt werden. Sobald Benutzer ihre Telefone einstecken, kann die Schadsoftware das Gerät sperren oder Anmeldedaten exportieren.

zIPS von Zimperium bietet eine Implementierung der Gerätesicherheit, um das Sicherheitsrisiko eines Benutzergeräts zu ermitteln. Anschließend wird anhand der Bedrohungslage festgestellt, ob ein Unternehmen diesem Gerät vertrauen kann. Selbst wenn Cyberkriminelle ihre Methoden weiterentwickeln, bietet zIPS die erforderliche Gerätebestätigung für die Implementierung von Zero Trust-Strategien für BYOD.

Die Vermeidung von Kompromittierungen mobiler Geräte ist eine wesentliche Voraussetzung für Zero Trust-Architekturen

Erfüllen mobile Geräte die Sicherheitsanforderungen eines Unternehmens nicht, beeinträchtigen diese die Zero Trust-Richtlinien.

Einer Studie von Zimperium zufolge halten 7 von 10 Unternehmen mobile Geräte in ihrem Betrieb für entscheidend. Die Mitarbeiter nutzen jedoch private mobile Geräte, um auf verschiedenste Daten zuzugreifen, von Kundenlisten und Kontostrategien bis hin zu Finanzmodellen. Diese Geräte greifen auf sensible Informationen zu und speichern diese, weshalb ein kompromittiertes mobiles Gerät zu erheblichen Datenverlusten führen kann.

Diese Geräte sind zudem oftmals das wichtigste Instrument des Unternehmens, um eine Multi-Faktor-Authentifizierung über SMS oder eine 2FA-App durchzuführen. Folglich kann ein kompromittiertes mobiles Gerät als Teil eines größeren Angriffs auf das Unternehmen verwendet werden, um die Anmeldedaten des Benutzers auszunutzen, die 2FA abzufangen und sich Zugriff zu verschaffen, wodurch Seitwärtsbewegungen begünstigt werden.

Zusammenfassend lässt sich sagen, dass ein kompromittiertes mobiles Gerät die Geräte- und Identitätssäulen von Zero Trust beeinträchtigen kann.

Verbe sserung der mobilen BYOD-Gerätesicherheit für die Implementierung der Zero Trust-Architektur

Die Integration von BYOD in eine Zero Trust-Architektur bringt viele Herausforderungen mit sich. Zwar bietet BYOD den Mitarbeitern mehr Flexibilität, schafft aber auch neue Sicherheitsrisiken. Unternehmen müssen MTD als Teil ihrer Zero Trust-Strategie einbeziehen, um die BYOD-Sicherheit zu verbessern.

Zimperium zIPS ist eine fortschrittliche Lösung zur Abwehr mobiler Gefahren für Unternehmen, die sowohl unternehmenseigene als auch BYOD-Geräte dauerhaft und direkt auf dem Gerät schützt. Die geräteinterne Sicherheit von Zimperium zIPS bietet Unternehmen die Integritätsbescheinigung für mobile Geräte, die für einen vollständigen Ansatz von Zero Trust erforderlich ist. Gleichzeitig schützt zIPS die Privatsphäre der Endbenutzer und sorgt dafür, dass Unternehmen die Zero Trust-Architektur (ZTA) und die Datenschutzrichtlinien einhalten.

Besuchen Sie www.zimperium.com/contact-us/, um sich eine Demo anzusehen und mehr über den Schutz Ihres Unternehmens vor mobilen Bedrohungen zu erfahren.