ZIMPERIUM.

Comment implémenter Mobile BYO dans un environnement Zero Trust

Le modèle de sécurité du réseau basé sur le périmètre qui définissait les utilisateurs à l'intérieur d'un périmètre de réseau d'entreprise comme étant « de confiance » ne fournit plus le même niveau de sécurité que par le passé. Aujourd'hui, le cloud computing, la mobilité et le travail à distance changent la façon dont les gens se connectent aux ressources numériques. Dans le cadre de ces nouveaux modèles, les employés veulent de plus en plus utiliser leurs propres appareils, rendant les politiques « Bring Your Own Device » (BYOD) encore plus critiques pour la sécurité. La mise en œuvre d'une architecture de type zero trust dans un environnement BYOD devrait intégrer la défense contre les menaces mobiles (MTD) pour augmenter la pile de technologie de sécurité.

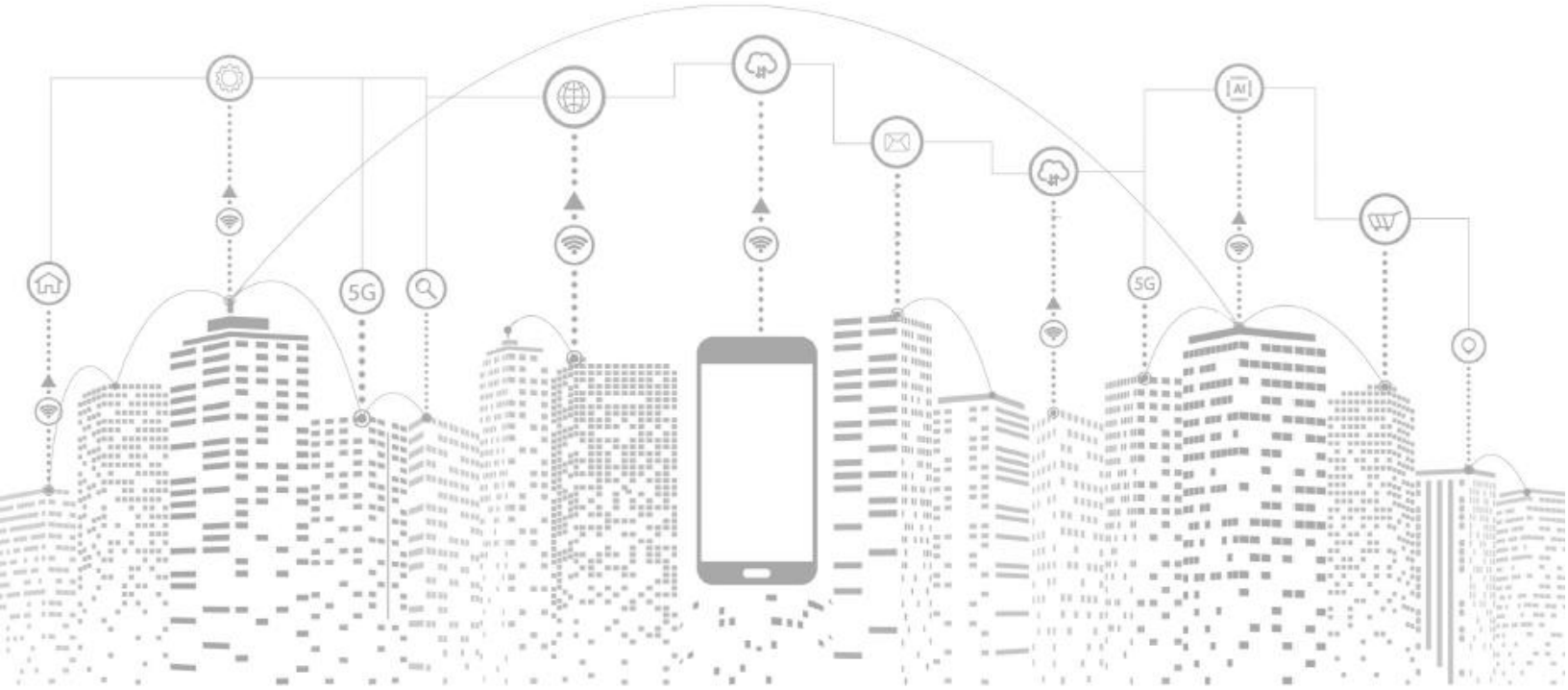
Pourquoi Zero Trust ?

Les nouvelles technologies et les nouveaux modèles de main-d' œuvre changent la façon dont les organisations doivent aborder la sécurité. Par exemple, une confiance inhérente existe lorsque tous les utilisateurs et appareils se connectent à des réseaux protégés.

Aujourd'hui, les gens utilisent l'internet public - même au sein des réseaux protégés - pour accéder aux applications Web afin de faire leur travail. En outre, les partenaires commerciaux tiers, comme les entrepreneurs, utilisent l'Internet public pour s'acquitter de leurs obligations.

Une approche de sécurité Zero Trust met l'accent sur la création d'un accès sécurisé aux ressources qui intègre :

- Attestation de santé du dispositif
- Protections au niveau des données
- Gestion des identités et des accès
- Segmentation stratégique du réseau



Pourquoi la conformité Zero Trust est difficile

À un niveau élevé, Zero Trust se concentre sur six piliers principaux :

Répondre à la conformité Zero Trust peut être très difficile parce que, au sein de chaque pilier, une entreprise doit sécuriser plusieurs choses. De plus, il existe très peu de processus étape par étape pour mettre en place une architecture de Zero Trust.

Par exemple, dans le pilier « Appareil », les entreprises doivent assurer une sécurité continue pour les postes de travail, les appareils mobiles (y compris les tablettes et les smartphones, les appareils IoT (comme les imprimantes et les serveurs).

Dans le cadre de ce pilier, les entreprises doivent gérer la sécurité des appareils en établissant des protections de base. En outre, ils ont besoin de visibilité sur la sécurité à l'avenir, ce qui signifie appliquer ces politiques et s'engager dans une attestation continue des risques de l'appareil.

Dans le cadre de la fonction de suivi de la conformité, il devrait ressembler à ceci :

- **Traditionnel :** Visibilité pour savoir si un périphérique est conforme aux politiques de sécurité établies
- **Avancé :** Capacité à faire respecter la conformité pour la plupart des appareils
- **Optimal :** Surveiller et valider la posture de sécurité de l'appareil en temps réel

Dans les environnements BYOD, de nombreuses entreprises auront du mal à savoir si un périphérique est conforme aux politiques de sécurité établies. Ils peuvent être incapables de contrôler quel appareil quelqu'un utilise ou ont du mal à répondre aux exigences de confidentialité lorsqu'ils tirent parti d'une technologie pour gagner en visibilité.

Chaque entreprise devrait fournir une protection contre ces menaces d'appareils mobiles

L'attestation continue de l'appareil est essentielle à une stratégie BYOD efficace pour répondre aux exigences de sécurité de Zero Trust. Lors de l'élaboration de ces stratégies et initiatives, les entreprises doivent tenir compte de diverses menaces qui peuvent nuire à leurs objectifs. Les employés utilisent constamment leurs appareils mobiles, et lorsqu'ils traversent le paysage, ils font face à de réelles menaces.

Hameçonnage (phishing)

L'accent accru mis sur les attaques par hameçonnage par les acteurs de la menace n'est pas nouveau. Selon un article de SC Media , les attaques d'hameçonnage basées en Russie ont été multipliées par huit entre le 27 février et le 1er mars 2022.

Selon notre rapport mondial sur les menaces mobiles 2022 (Global Mobile Threat Report) , 55 % des personnes interrogées ont déclaré que « l'exploitation par hameçonnage » était leur principal risque, 61 % affirmant avoir vu une augmentation des attaques d'hameçonnage pendant la pandémie de la COVID-19.

Alors que la plupart du temps, les utilisateurs finaux ne veulent jamais vraiment causer de mal, la sophistication et le barrage accrus des activités rendent difficile de trier le blé numérique de la balle. Les solutions antivirus ou d'hameçonnage traditionnelles basées sur la signature constituent un point de départ. Pourtant, beaucoup d'entre eux sont de nature réactive et ne répondent pas adéquatement au défi du volume de nouveaux sites d'hameçonnage qui se lèvent chaque seconde.

Plus inquiétant, les chercheurs de Zimperium ont détecté une augmentation des sites Web d'hameçonnage spécifiques aux mobiles. Après avoir analysé nos données et les données publiques basées sur deux ans, le nombre de sites Web d'hameçonnage spécifiques aux mobiles a augmenté de 50 %. En outre, au cours de 2021, 75 % des sites d'hameçonnage ont analysé des appareils mobiles spécifiquement ciblés et ont fourni un contenu approprié au format mobile.

Par exemple, les agresseurs ont ciblé les appareils mobiles avec les deux techniques suivantes :

- **Sites Web adaptatifs :** Selon l'appareil utilisé, les sites Web adaptatifs peuvent charger différents contenus et les rediriger vers d'autres sites. En adaptant le contenu en fonction de l'agent utilisateur d'un point terminal mobile, les agresseurs peuvent cibler exclusivement des dispositifs mobiles.
- **Sites Web réactifs :** Étant donné que ceux-ci adaptent la taille et le placement des objets en fonction de la taille de l'écran du point de terminaison, les agresseurs peuvent utiliser ces fonctionnalités légitimes pour cibler les appareils mobiles.

Les appareils mobiles offrent une couche de complexité supplémentaire qui rend les approches traditionnelles d'antivirus et d'hameçonnage inadéquates pour les appareils mobiles. Tout d'abord, la connectivité d'un périphérique à un cloud, en plus des considérations de confidentialité et de latence, rend toute approche cloud prioritaire impossible à la fois du point de vue de la sécurité technique et opérationnel. En outre, les appareils mobiles ne peuvent pas télécharger ou prendre en charge de gros fichiers de signature, de sorte que toute dépendance à des bases de données connues, ou des flux de menaces, est inadéquate et impossible.

Cela signifie que les seules options viables pour protéger les appareils mobiles doivent être en mesure de le faire sur l'appareil sans aucune dépendance sur le cloud et doivent être en mesure de détecter les menaces connues et inconnues sans avoir à les avoir vues auparavant. Le moteur de détection z9 de Zimperium utilisant ses classificateurs d'apprentissage automatique (ML) adapte ce projet de loi non seulement à l'hameçonnage, mais aussi aux menaces liées aux appareils, aux réseaux et aux applications.

Applications téléchargées

De nombreuses organisations connaissent déjà les risques que l'informatique fantôme peut causer sur les appareils traditionnels. Cependant, l'impossibilité d'ajouter ces applications aux inventaires d'actifs conduit à un manque de visibilité.

Les applications téléchargées sur les appareils mobiles deviennent encore plus risquées. Les membres de l'équipe utilisent des appareils mobiles personnellement et professionnellement, ce qui empêche les organisations de contrôler la sécurité des applications qu'elles utilisent pour gérer leur utilisation personnelle.

La convergence des applications mobiles/applications de bureau dans le système d'exploitation moderne est une tendance qui permet aux acteurs de la menace d'utiliser plus facilement les appareils mobiles comme porte dérobée dans les systèmes et les réseaux. Selon les données du rapport sur les menaces de Zimperium, 42 % des entreprises ont signalé des applications et des ressources non autorisées pour accéder aux données de l'entreprise.

La solution MTD de Zimperium est explicitement dédiée à la prévention des menaces, à la détection et à la réponse pour les appareils exécutant iOS, Android et Chrome OS. Alors qu'une solution de gestion des appareils mobiles (MDM) peut aider à l'administration et à l'application des politiques, la MTD de Zimperium protège l'organisation en compartimentant les informations et les processus sensibles, réduisant ainsi la surface d'attaque.

Logiciels malveillants à l'intérieur des applications téléchargées

Puisque la surface d'attaque mobile diffère de la surface d'attaque traditionnelle, les logiciels malveillants mobiles sont également uniques. Parfois, l'application est le malware, tandis que d'autres fois, les attaquants utilisent des applications pour livrer le malware via une vulnérabilité.

Applications malveillantes

En 2021, l'analyse de sécurité mobile de Zimperium a révélé 2 034 217 nouveaux échantillons de logiciels malveillants détectés dans la nature. En moyenne, cela représente près de 36 000 nouvelles variantes de logiciels malveillants par semaine - plus de 5 000 par jour. Par exemple, les agresseurs ont ciblé les utilisateurs d'appareils mobiles pendant la saison des fêtes 2021 avec des SMS et des liens e-mail promouvant les réductions, en espérant que les gens les utiliseraient pour télécharger une application malveillante.

Alors que certaines variantes de logiciels malveillants mobiles agissent comme des attaques de point de terminaison traditionnelles, d'autres regardent et agissent différemment. Par exemple, certains peuvent :

- Voler les identifiants d'authentification à deux facteurs (2FA) par SMS ou notifications d'application.
- Effectuez des attaques de superposition lorsqu'un utilisateur entre des informations d'identification dans une application secondaire qu'il estime légitime.
- Surveillez les autres applications installées grâce aux autorisations du service d'accessibilité.
- Utilisez le suivi de position via les services GPS.
- Activez les caméras ou les microphones pour enregistrer audio et vidéo.
- Accédez à des contenus sensibles tels que des photos, des contacts ou des données personnelles.
- Capturez et suivez les données du capteur.

Applis risquées

En tant que technologie plus récente, les applications mobiles peuvent ne pas avoir le même niveau de sécurité intégré dans leur cycle de développement de logiciels, d'autant plus que les entreprises essaient de pousser de nouvelles expériences rapidement.

Au cours du second semestre 2021, Zimperium a constaté qu'environ 81 % des plus de 160 applications mobiles financières mondiales ont recherché et analysé des données potentiellement sensibles. Au-delà des applications financières, Zimperium a constaté que 77 % des applications Android et 46 % des applications iOS de soins de santé, de vente au détail et de style de vie utilisaient ou utilisaient potentiellement au moins un algorithme de chiffrement vulnérable.

En d'autres termes, même lorsque les utilisateurs finaux téléchargent des applications légitimes, ils peuvent créer des risques qui ont un impact sur l'entreprise. Alors que la sécurité du développement des applications mobiles en est encore à ses débuts, les entreprises doivent réfléchir à la manière dont elles se protègent de ces risques.

Attaques de réseau

Travailler de partout signifie que les employés se connectent à des WiFis non sécurisés. Bien que ce ne soit pas nouveau, les attaques de l'homme au milieu (MitM) restent efficaces, avec les recherches de Zimperium constatant que 13 % des appareils ont rencontré des attaques MitM.

Tout aussi problématique, auparavant « protégé » WiFis peut être sapé par des attaques jumeaux maléfiques où les acteurs malveillants usurpent un WiFi gratuit qui utilise un portail pour l'entrée, comme dans un hôtel ou un aéroport. D'après les recherches de Zimperium, environ 16 % des appareils mobiles ont rencontré un réseau malveillant connu, une manipulation du trafic ou un point d'accès malhonnête. Cela dit, les utilisateurs finaux qui se sont précédemment connectés au vrai WiFi sont plus susceptibles de croire qu'il est sécurisé. Cependant, lorsque l'utilisateur se connecte au portail de l'entreprise via ce faux WiFi, les acteurs malveillants peuvent voler leurs identifiants.

Avec Zimperium, les entreprises peuvent appliquer les exigences d'accès conditionnel lorsque les personnes changent d'emplacement parce que l '« état » de l'appareil est surveillé en permanence. Avec la solution MTD de Zimperium , l'entreprise bénéficie d'une visibilité sur la sécurité des appareils et peut plus adéquatement refuser l'accès à partir d'une connexion WiFi non autorisée.

Stations de charge

Lorsque les entreprises considèrent les risques mobiles, elles s'inquiètent souvent le plus de l'hameçonnage. Cependant, se concentrer uniquement sur l'hameçonnage ne prend pas en compte d'autres méthodes de livraison de logiciels malveillants.

Récemment, la FCC a averti les consommateurs que les bornes de recharge USB publiques , comme celles des centres commerciaux et des aéroports, étaient exploitées par des cybercriminels. Ce type d'attaque, connu sous le nom de « jus jacking », peut être exécuté via le port USB ou un câble laissé par les cybercriminels. Lorsque les utilisateurs branchent leurs téléphones, le logiciel malveillant peut verrouiller un appareil ou exporter des informations d'identification.

Zimperium zIPS fournit une implémentation de sécurité sur l'appareil pour comprendre le risque de l'appareil d'un utilisateur. La posture de menace fournit alors l'attestation nécessaire pour déterminer si une entreprise doit faire confiance à cet appareil. Même à mesure que les cybercriminels développent leurs méthodologies, zIPS offre l'attestation de périphérique nécessaire pour mettre en œuvre des stratégies de confiance zéro pour BYOD.

Empêcher le compromis des appareils mobiles est fondamental pour les architectures Zero Trust

Si les appareils mobiles ne répondent pas aux exigences de sécurité d'une organisation, ils sapent ses politiques de confiance zéro.

Selon les recherches de Zimperium, 7 organisations sur 10 considèrent que les appareils mobiles sont essentiels à leurs opérations. Cependant, les employés utilisent des appareils mobiles personnels pour accéder à tout, des listes de clients et des stratégies de compte aux modèles financiers. Comme ces accès et stocker des informations sensibles, un appareil mobile compromis peut conduire à une violation de données.

En outre, ces appareils sont souvent le principal moyen de l'organisation de mettre en œuvre l'authentification multifactorielle par SMS ou une application 2FA. En conséquence, un dispositif mobile compromis peut être utilisé dans le cadre d'une attaque plus importante contre l'organisation, tirant parti des informations d'identification de l'utilisateur, interceptant le 2FA et obtenant un accès qui permet un mouvement latéral.

En bref, un appareil mobile compromis peut saper les piliers de l'appareil et de l'identité de Zero Trust.

Amélioration de la sécurité des appareils mobiles BYOD pour la mise en œuvre d'une architecture Zero Trust

L'intégration de BYOD dans une architecture Zero Trust pose de nombreux défis. Bien que le BYOD offre une plus grande flexibilité aux employés, il crée également de nouveaux risques pour la sécurité. Les entreprises doivent inclure MTD dans leurs stratégies Zero Trust pour améliorer la sécurité BYOD.

Zimperium zIPS est une solution avancée de défense contre les menaces mobiles pour les entreprises, fournissant une protection persistante sur l'appareil aux appareils appartenant à l'entreprise et aux appareils BYOD. La sécurité de Zimperium zIPS sur l'appareil fournit aux entreprises l'attestation d'intégrité de l'appareil mobile nécessaire pour une approche complète de Zero Trust. De plus, par sa conception, zIPS protège la vie privée des utilisateurs finaux, en veillant à ce que les entreprises se conforment aux mandats Zero Trust Architecture (ZTA) et de confidentialité.

Pour voir une démo et en savoir plus sur la protection de votre entreprise contre les menaces mobiles, visitez www.zimperium.com/contact-us/ .