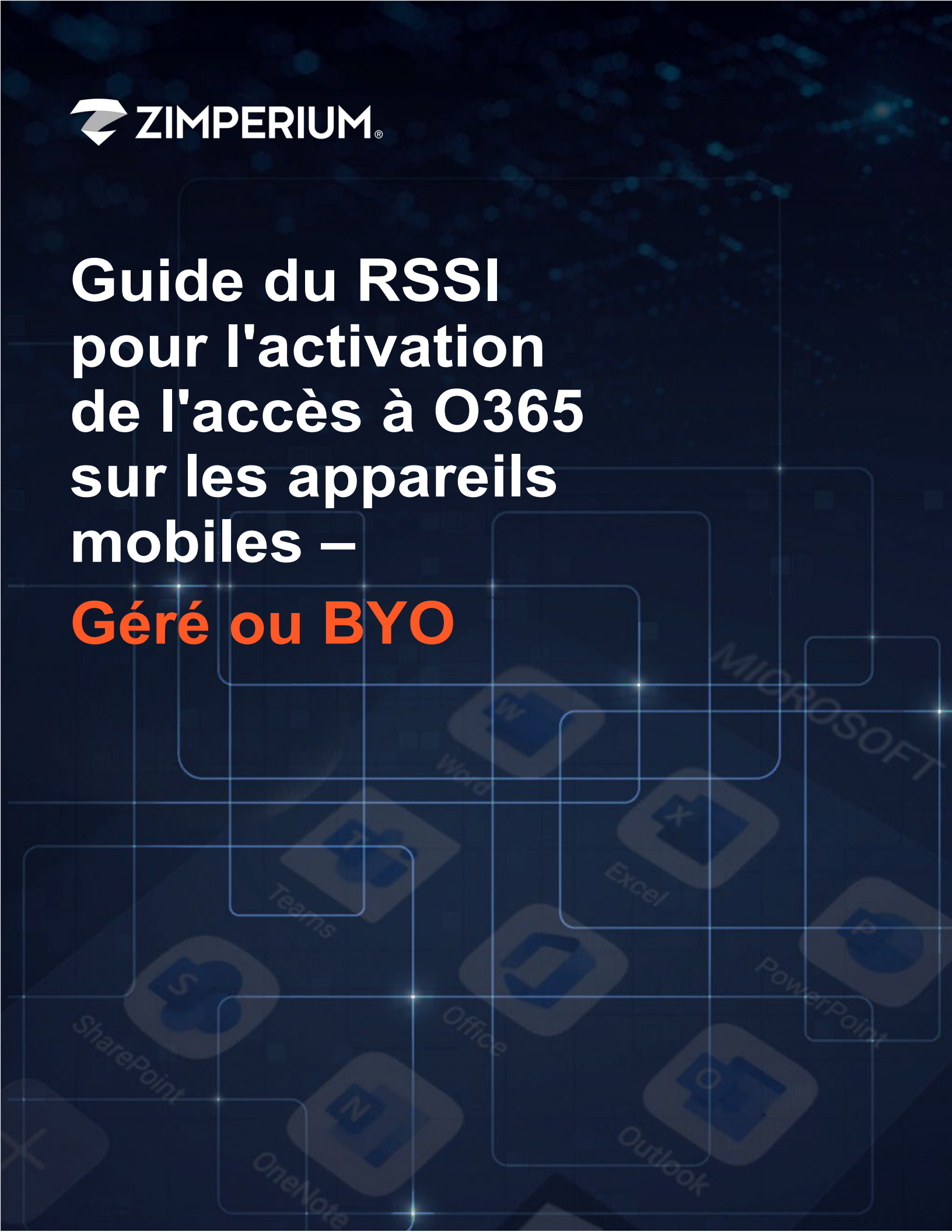
ZIMPERIUM®

Guide du RSSI pour l'activation de l'accès à O365 sur les appareils mobiles – Géré ou BYO



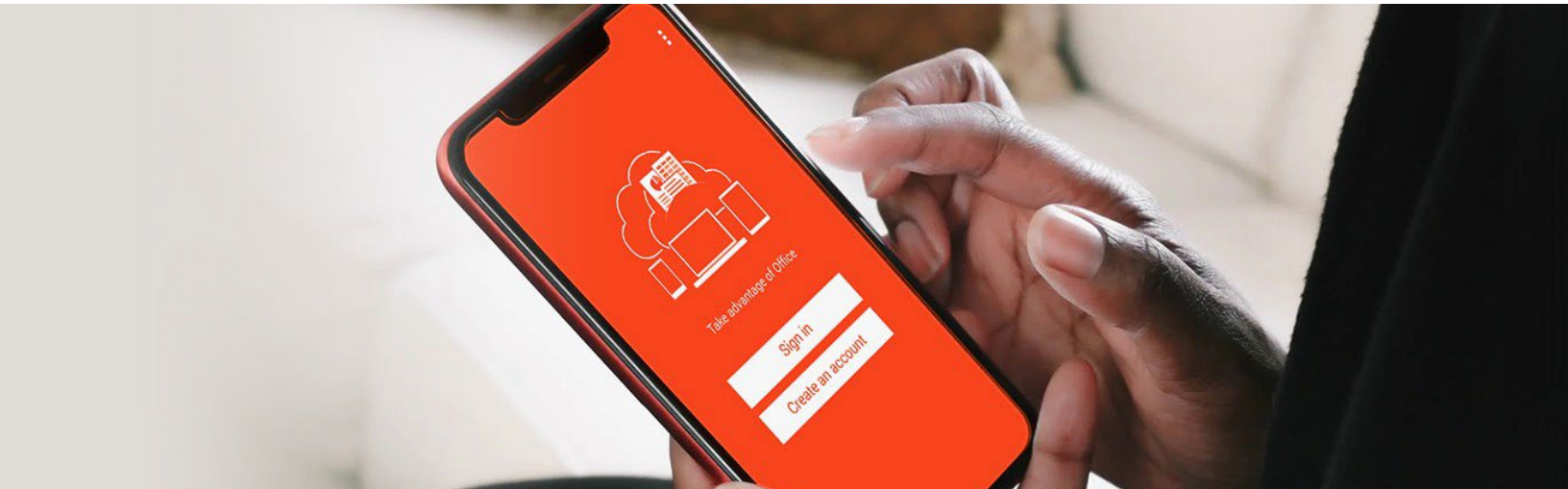
Introduction

Environ 84 % des organisations ont activé Office 365 (O365) sur les appareils mobiles de leurs employés, mais plus de 50 % n'ont pas déployé de solutions de défense contre les menaces mobiles (MTD) pour les empêcher d'être compromis[1]. C'est pourquoi nous avons demandé à Eric Green, spécialiste de la protection des opérations commerciales chez TikTok, de partager avec nous sa vision de ce que les organisations devraient faire dès maintenant pour s'assurer que l'accès mobile à O365 soit à la fois transparent et sécurisé.

Z (Zimperium) : Faisons tout d'abord le point en définissant le contexte entourant ce sujet, car sécuriser efficacement l'accès mobile à O365 était déjà un défi avant même que la pandémie ne frappe. Quels étaient l'environnement et le sentiment qui vous animait, vous et votre équipe, lorsque le confinement a été décrété pour la première fois en mars 2020 ?

Eric: J'en étais à mon huitième mois en tant que responsable mondial de la sécurité mobile et Mac chez HSBC. Personne n'était prêt à relever les énormes défis opérationnels et sécuritaires auxquels nous allions bientôt être confrontés. Presque du jour au lendemain, nous avons constaté une augmentation massive du nombre d'employés ayant besoin d'un accès mobile à O365. C'était problématique puisque **O365 sur mobile donne aux utilisateurs le même niveau d'accès aux données d'entreprise exclusives et personnelles que les ordinateurs de bureau et les ordinateurs portables entièrement sécurisés.** Nous avons dû agir très rapidement pour nous assurer que l'accès serait sécurisé. Heureusement, nous avions déjà une stratégie MTD solide en place.

[1] Réponses au sondage rapide, décembre 2021 et janvier 2022 - home.pulse.qa-



Z: Comment vos pairs d'autres entreprises géraient-ils la sécurité de l'accès mobile à O365?

Eric: La plupart des organisations ont adopté l'approche traditionnelle, déployant des solutions UEM (y compris MDM et MAM) comme Microsoft Intune pour contrôler l'accès à O365 et à d'autres ressources à partir de téléphones mobiles, de tablettes et d'ordinateurs portables.

Les solutions UEM offrent la visibilité nécessaire pour surveiller et appliquer les politiques d'authentification des utilisateurs, d'accès aux données et d'utilisation acceptable. Lorsqu'un niveau de risque est dépassé, ils peuvent également appliquer des mesures de secours automatisées, tels que la désactivation d'une application O365, l'effacement de l'appareil ou sa mise hors ligne. **Mais les solutions UEM ne peuvent pas détecter les attaques sophistiquées de type hameçonnage ou celles émanant de logiciels malveillants, d'appareils et de réseaux.** Le risque encouru par les entreprises s'est accru de manière exponentielle avec l'augmentation rapide du nombre d'appareils appartenant aux employés. La pandémie a considérablement élargi la surface d'attaque qui était déjà vaste, vulnérable et extrêmement difficile à surveiller et à sécuriser.

Z: Certaines organisations ont suggéré que les VPN pouvaient aider à sécuriser O365 sur mobile. Pourquoi n'offrent-ils pas une protection suffisante?

Eric: Les VPN sont efficaces dans les situations « point à point », où il faut chiffrer le trafic entre les appareils mobiles et les ressources locales de l'entreprise. **Mais les VPN ne peuvent pas détecter les menaces mobiles ni y faire face.** Ils sont moins adaptés dans les situations où vous accédez aux services du cloud avec un navigateur, en particulier si vous devez effectuer des liaisons terrestres avant d'envoyer les données vers le cloud. Cela augmente rapidement les coûts liés au réseau et ralentit les performances des utilisateurs. Les outils des VPN ne sont pas non plus infaillibles. Et si un individu malveillant vole les informations d'identification VPN d'un employé, il acquiert le même niveau d'accès au réseau de l'entreprise. Les solutions MTD peuvent aider à prévenir lesdites violations de données en détectant les situations à risque et en informant les utilisateurs que leurs identifiants sont susceptibles d'avoir été volés.

Les solutions MTD peuvent aider à prévenir lesdites violations de données en détectant les situations à risque et en informant les utilisateurs que leurs identifiants sont susceptibles d'avoir été volés.

Z: Qu'en est-il de Microsoft Defender pour Endpoint ? Quelle est son efficacité face aux risques de sécurité rencontrés par O365 mobile?

Eric: Il y a des avantages et des inconvénients. Un des aspects positifs est l'intégration fluide entre les produits Microsoft. Par exemple, il est possible d'établir une connexion de service à service entre Defender et Intune pour partager des données et des profils d'appareil. Cela vous permet de définir des niveaux de risque dans Defender, lesquels déclenchent à leur tour des contrôles d'accès conditionnels dans Intune. **Cependant, Defender est un produit relativement récent et ses fonctionnalités MTD sont primitives.** Par exemple, Defender ne fournit pas suffisamment d'informations sur l'état d'un appareil mobile pour déterminer avec précision s'il est digne de confiance, débridé ou compromis. Les solutions MTD matures offrent des capacités plus complètes permettant de détecter les menaces et de faire face automatiquement à celles-ci au niveau de l'utilisateur, de l'appareil, de l'application et du réseau. Ils fournissent également aux analystes les données techniques et télémétriques dont ils ont besoin pour analyser les causes profondes des menaces en question et traquer celles-ci..

La flexibilité et la pérennité sont essentielles. Les solutions MTD doivent s'intégrer facilement à votre SIEM, à votre fournisseur d'identité et à vos autres investissements en matière de sécurité.

« Defender ne fournit pas suffisamment d'informations sur l'état d'un appareil mobile pour déterminer avec précision s'il est digne de confiance, débridé ou compromis »

Z: Comment MTD répond aux initiatives Zero Trust que de nombreuses organisations ont accélérées en raison du COVID?

Eric: Le modèle Zero Trust exige que les utilisateurs, les appareils, les réseaux et les applications prouvent qu'ils sont dignes de confiance avant de leur accorder l'accès à des ressources telles que O365. Le défi consiste à mettre en œuvre Zero Trust sans que les administrateurs n'aient à surveiller chaque interaction ni à forcer les employés à passer par des démarches compliquées pour effectuer des tâches de base.

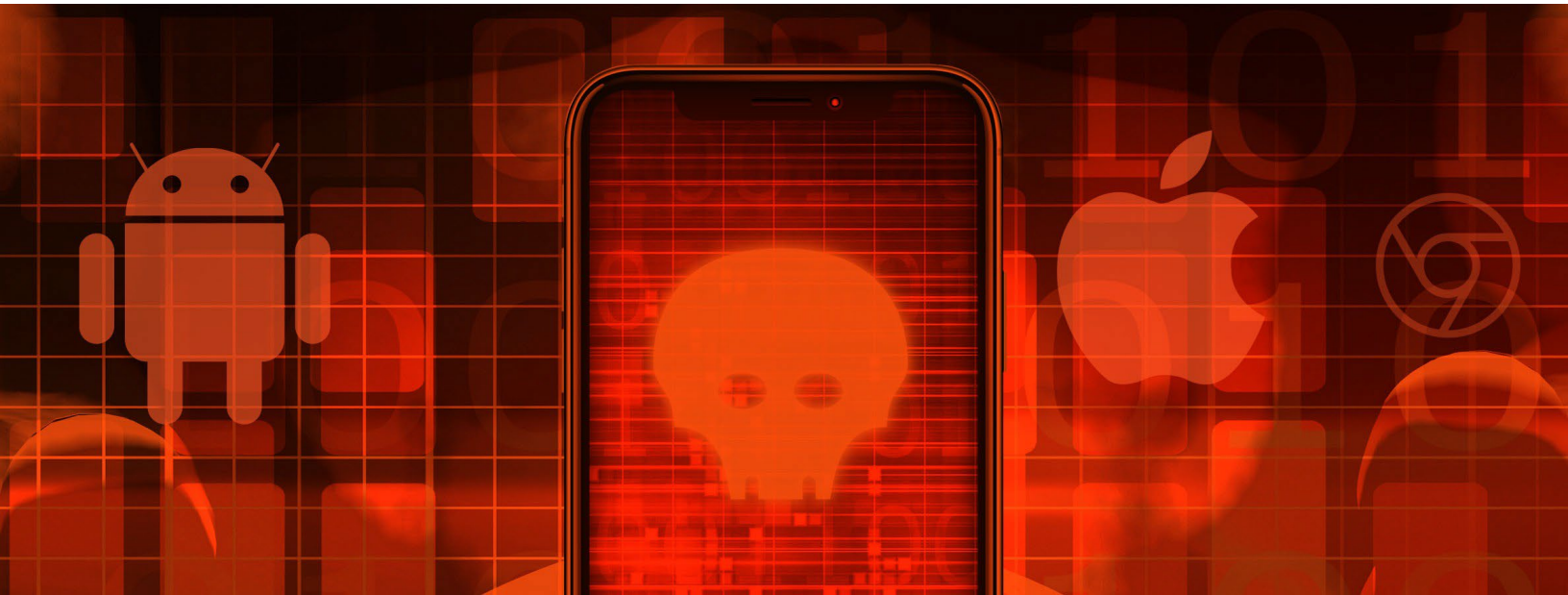
MTD fonctionne bien dans un environnement Zero Trust car il surveille en permanence l'appareil mobile pour détecter les logiciels malveillants, exploits d'hameçonnage, points d'accès malveillants, applications chargées en marge et autres menaces potentielles. Si un employé n'agit pas de manière malveillante ou qu'il ne met pas son appareil mobile en danger par nadvertance, alors son accès aux ressources reste intact. Si MTD détecte une menace ou un risque potentiel, la menace peut être neutralisée immédiatement, et l'appareil est alors ramené à un état où il est certifié comme étant digne de confiance..

Z: Comment les différences entre iOS et Android influencent-elles votre approche pour sécuriser O365 dans un environnement hybride?

Eric: Les outils et les flux de travail sont différents, mais les objectifs restent les mêmes. Les profils de travail gérés par Android séparent les applications et les données professionnelles des applications et des données personnelles. Cela permet de définir et de mettre en œuvre des politiques de conformité des appareils au niveau des applications professionnelles, lesquelles sont appliquées de manière continue, que l'appareil se connecte à un service basé sur le cloud comme O365 ou bien que celui-ci se connecte à une base de données située derrière le pare-feu de l'entreprise. Cela permet de réduire les risques liés aux appareils BYO sans violer la vie privée des employés. Apple essaie de rattraper son retard avec son Gestionnaire de profils. Un jour ou l'autre, les deux produits se vaudront.

Mais sinon, les différences entre les systèmes d'exploitation n'ont pas d'importance. Une solution MTD efficace se doit de détecter les menaces et de les neutraliser, et ce que l'appareil exécute iOS, Android ou bien ChromeOS (sur Chromebooks). La puissance de l'apprentissage automatique consiste à détecter les menaces en fonction de leurs caractéristiques bien précises et des flux de processus. L'important est de déployer ces modèles et leur logique de détection et d'intervention localement sur chaque appareil mobile (détection au niveau de l'appareil). Un danger peut survenir en quelques millisecondes. On ne peut pas se permettre le temps de latence qui accompagne les recherches sur le cloud et les correspondances de signature.

« Une solution MTD efficace se doit de détecter les menaces et de les neutraliser, et ce que l'appareil exécute iOS, Android ou bien ChromeOS (sur Chromebooks). »



Z: Que pensez-vous des bonnes pratiques en matière de gestion des correctifs ? Quelle était votre approche dans ce domaine?

Eric: Les utilisateurs n'aiment pas qu'on leur dise d'installer des correctifs, surtout si l'appareil mobile leur appartient personnellement. Beaucoup ne les installent pas ou attendent la dernière minute pour le faire, c'est-à-dire lorsqu'ils sont sur le point de perdre leur accès aux ressources de l'entreprise. Certains appareils mobiles ne peuvent pas installer des correctifs car ils sont obsolètes. Il faut établir des priorités. Les mises à jour des systèmes d'exploitation sont cruciales car elles fournissent souvent des correctifs de sécurité pour remédier aux vulnérabilités critiques. La mise à jour d'une application est généralement moins urgente, sauf s'il s'agit d'une application officielle de l'entreprise, comme Slack, que les employés doivent impérativement utiliser pour être productifs.

Cela se complique lorsqu'il y a un mélange d'appareils iOS et Android. Les utilisateurs d'Apple ont tendance à être rigoureux. Ils ont l'habitude d'installer des correctifs et des mises à jour régulièrement. L'écosystème Android est beaucoup plus fragmenté. Les fabricants de matériel et les opérateurs sans fil contrôlent souvent le calendrier et la disponibilité des correctifs et des versions du système d'exploitation. Au final, c'est un exercice d'équilibriste. Il faut hiérarchiser les correctifs en fonction des risques bien précis encourus par votre organisation et des exigences particulières des différents types d'utilisation. Il n'y a pas de solution parfaite. Les correctifs sont toujours mis en place au cas par cas. **C'est pourquoi il faut disposer d'une solution capable de détecter les individus malveillants et de les empêcher d'activer des logiciels malveillants et d'exploiter les vulnérabilités de chaque appareil mobile, et ce quel que soit le modèle de l'appareil ou le niveau de conformité.**

Z: En résumé, compte tenu du contexte actuel en matière de menace, quelles recommandations adresseriez-vous aux RSSI pour les conseiller sur la manière de sécuriser l'accès mobile à O365?

Eric: Sécuriser l'accès mobile à O365 est essentiel mais, honnêtement, il s'agit d'une pièce d'un puzzle beaucoup plus grand. Les employés vont continuer à accéder à l'ensemble des ressources de l'entreprise à partir d'appareils mobiles. Les groupes de pirates informatiques continueront à trouver de nouvelles façons de les piéger en leur faisant commettre des erreurs et à exploiter les vulnérabilités des applications mobiles et des systèmes d'exploitation. La clé consiste à identifier et à traiter en priorité les menaces mobiles qui présentent les risques les plus importants pour votre organisation.

Si vous utilisez Intune, assurez-vous que vos politiques de gestion des appareils prennent en compte ces risques sans être trop restrictives. Formez les utilisateurs à adopter de bonnes habitudes en matière de sécurité informatique. Assurez-vous que les navigateurs utilisent un chiffrement approprié pour accéder aux services du cloud. Accélérez votre transition vers la politique Zero Trust. Cela recouvre les opérations de blocage et de résolution de base.

Mais vous devez également déployer une solution MTD qui s'avère efficace pour détecter et atténuer les menaces mobiles auxquelles sont confrontées les utilisateurs, les appareils, les réseaux et les applications. Assurez-vous que la solution que vous choisissez fonctionne bien avec votre infrastructure de gestion/sécurité existante et que celle-ci préserve la flexibilité nécessaire pour répondre aux besoins de votre infrastructure qui évolue de manière constante pour faire face aux nouveaux défis en matière de sécurité.