Sécurité basée sur les hôtes

Ayoub Abdellaoui

India_S3

Introduction

- Les hôtes d'administration sécurisés sont des stations de travail ou des serveurs qui ont été configurés spécifiquement pour créer des plateformes sécurisées à partir desquelles les comptes privilégiés peuvent effectuer des tâches d'administration dans Active Directory ou sur des contrôleurs de domaine, des systèmes joints à un domaine et des applications s'exécutant sur des systèmes joints à un domaine. Dans ce cas, les « comptes privilégiés » font référence non seulement aux comptes qui sont membres des groupes les plus privilégiés dans Active Directory, mais également à tous les comptes qui ont été délégués avec des droits et des autorisations qui permettent d'effectuer des tâches administratives.

Introduction

- Ces comptes peuvent être des comptes de support technique qui ont la possibilité de réinitialiser les mots de passe de la plupart des utilisateurs d'un domaine, des comptes qui sont utilisés pour administrer des enregistrements et des zones DNS ou des comptes utilisés pour la gestion de la configuration. Les hôtes d'administration sécurisés sont dédiés aux fonctionnalités administratives. Ils n'exécutent pas de logiciels tels que des applications de messagerie, des navigateurs web ou des logiciels de productivité comme Microsoft Office.
- Bien que les comptes et groupes « les plus privilégiés » soient donc les plus strictement protégés, cela n'élimine pas la nécessité de protéger tous les comptes et groupes auxquels des privilèges supérieurs à ceux des comptes d'utilisateur standard ont été accordés.

Introduction

- Un hôte d'administration sécurisé peut être une station de travail dédiée qui est utilisée uniquement pour les tâches administratives, un serveur membre qui exécute le rôle serveur de passerelle Bureau à distance et auquel les utilisateurs informatiques se connectent pour effectuer l'administration des hôtes de destination, ou un serveur qui exécute le rôle Hyper-V et fournit une machine virtuelle unique que chaque utilisateur informatique pourra utiliser pour ses tâches d'administration. Dans de nombreux environnements, il est possible de mettre en place des combinaisons des trois approches.

Introduction

- L'implémentation d'hôtes administratifs sécurisés nécessite une planification et une configuration cohérentes avec la taille, les pratiques administratives, l'appétence au risque et le budget de votre organisation. Vous trouverez ici des considérations et des options pour l'implémentation d'hôtes d'administration sécurisés que vous pouvez utiliser pour développer une stratégie administrative adaptée à votre organisation.

Principes de création d'hôtes d'administration sécurisés

- Pour sécuriser efficacement les systèmes contre les attaques, il convient de garder à l'esprit quelques principes généraux :
  - Vous ne devez jamais administrer un système approuvé (comme un serveur sécurisé de type contrôleur de domaine) à partir d'un hôte moins approuvé (comme une station de travail qui n'est pas sécurisée au même degré que les systèmes qu'elle gère).
  - Ne vous fiez pas à un seul facteur d'authentification pour exécuter des activités privilégiées, autrement dit, les combinaisons de nom d'utilisateur et de mot de passe ne doivent pas être considérées comme une authentification acceptable, car elles ne représentent qu'un seul facteur (quelque chose que vous connaissez). Vous devez prendre en compte l'emplacement où les informations d'identification sont générées et mises en cache ou stockées dans des scénarios d'administration.
  - Bien que la plupart des attaques dans le paysage actuel des menaces tirent parti des programmes malveillants et du piratage malveillant, n'omettez pas la sécurité physique lors de la conception et de l'implémentation d'hôtes d'administration sécurisés.

Configuration de compte

- Même si votre organisation n'utilise pas actuellement de cartes à puce, vous devez envisager de les implémenter pour les comptes privilégiés et les hôtes administratifs sécurisés. Les hôtes administratifs doivent être configurés pour exiger une ouverture de session par carte à puce pour tous les comptes en modifiant le paramètre suivant dans un objet de stratégie de groupe lié aux unités d'organisation contenant des hôtes d'administration :

- Configuration ordinateur\Stratégies\Paramètres Windows\Stratégies locales\Options de sécurité\Ouverture de session interactive : Exiger une carte à puce

- Ce paramètre nécessite que toutes les ouvertures de session interactives utilisent une carte à puce, quelle que soit la configuration d'un compte individuel dans Active Directory.

Configuration de compte

- Vous devez également configurer des hôtes d'administration sécurisés pour autoriser les ouvertures de session uniquement par des comptes autorisés, qui peuvent être configurés dans :

- Configuration ordinateur\Stratégies\Paramètres Windows\Paramètres de sécurité\Stratégies locales\Affectation des droits utilisateur

- Vous accordez ainsi des droits d'ouverture de session interactifs (et, le cas échéant, des services Bureau à distance) uniquement aux utilisateurs autorisés de l'hôte d'administration sécurisé.

Sécurité physique

- La sécurité physique inclut le contrôle de l'accès physique aux hôtes d'administration. Dans une petite organisation, cela peut signifier que vous maintenez une station de travail d'administration dédiée verrouillée dans un bureau ou un tiroir de bureau lorsqu'elle n'est pas utilisée. Cela peut également signifier que lorsque vous devez effectuer l'administration d'Active Directory ou de vos contrôleurs de domaine, vous vous connectez directement au contrôleur de domaine.

Sécurité physique

- Dans les organisations de taille moyenne, vous pouvez envisager d'implémenter des « serveurs de rebond » administratifs sécurisés qui se trouvent dans un emplacement sécurisé d'un bureau et qui sont utilisés lorsque la gestion d'Active Directory ou de contrôleurs de domaine est requise. Vous pouvez également implémenter des stations de travail d'administration qui sont verrouillées dans des emplacements sécurisés lorsqu'elles ne sont pas utilisées, avec ou sans serveurs de rebond.
- Dans les grandes organisations, vous pouvez déployer des serveurs de rebond hébergés dans un centre de données qui fournissent un accès strictement contrôlé à Active Directory, des contrôleurs de domaine et des serveurs de fichiers, d'impression ou d'applications. L'implémentation d'une architecture de serveur de rebond est susceptible d'inclure une combinaison de stations de travail et de serveurs sécurisés dans des environnements volumineux.

Sécurité physique

- Quelle que soit la taille de votre organisation et la conception de vos hôtes d'administration, vous devez sécuriser les ordinateurs physiques contre l'accès non autorisé ou le vol, et utiliser le chiffrement de lecteur BitLocker pour chiffrer et protéger les lecteurs sur les hôtes d'administration. En implémentant BitLocker sur des hôtes d'administration, même si un hôte est volé ou si ses disques sont supprimés, vous pouvez vous assurer que les données du lecteur sont inaccessibles aux utilisateurs non autorisés.

Versions et configuration du système d'exploitation

- Tous les hôtes d'administration, qu'il s'agisse de serveurs ou de stations de travail, doivent exécuter le système d'exploitation le plus récent utilisé dans votre organisation pour les raisons décrites auparavant. En exécutant les systèmes d'exploitation actuels, votre personnel administratif bénéficie de nouvelles fonctionnalités de sécurité, d'une prise en charge complète du fournisseur et de fonctionnalités supplémentaires introduites dans le système d'exploitation. En outre, lorsque vous évaluez un nouveau système d'exploitation, en le déployant d'abord sur des hôtes d'administration, vous devez vous familiariser avec les nouvelles fonctionnalités, les nouveaux paramètres et mécanismes de gestion qu'il offre, avant de pouvoir les exploiter dans la planification d'un déploiement plus large du système d'exploitation. D'ici là, les utilisateurs les plus chevronnés de votre organisation seront également ceux qui connaissent le nouveau système d'exploitation et qui sont les mieux placés pour le prendre en charge.

Assistant Configuration de la sécurité de Microsoft

- Si vous implémentez des serveurs de rebond dans le cadre de votre stratégie d'hôte d'administration, vous devez utiliser l'Assistant Configuration de la sécurité intégré pour configurer les paramètres de service, de registre, d'audit et de pare-feu afin de réduire la surface d'attaque du serveur. Une fois que les paramètres de configuration de l'Assistant Configuration de la sécurité ont été collectés et configurés, ils peuvent être convertis en un objet de stratégie de groupe utilisé pour appliquer une configuration de base de référence cohérente sur tous les serveurs de rebond. Vous pouvez modifier davantage l'objet de stratégie de groupe pour implémenter des paramètres de sécurité spécifiques aux serveurs de rebond et combiner tous les paramètres avec des paramètres de base supplémentaires extraits du Microsoft Security Compliance Manager.

Microsoft Security Compliance Manager

- Microsoft Security Compliance Manager est un outil gratuit qui intègre des configurations de sécurité recommandées par Microsoft, en fonction de la version du système d'exploitation et de la configuration du rôle, et les collecte dans un outil et une interface utilisateur uniques qui peuvent être utilisés pour créer et configurer des paramètres de sécurité de base pour les contrôleurs de domaine. Les modèles de Microsoft Security Compliance Manager peuvent être combinés avec les paramètres de l'Assistant Configuration de la sécurité pour produire des bases de référence de configuration complètes pour les serveurs de rebond déployés et appliqués par les objets de stratégie de groupe déployés sur les unités d'organisation dans lesquelles les serveurs de rebond se trouvent dans Active Directory.

AppLocker

- Les hôtes d'administration et les machines virtuelles doivent être configurés avec des scripts, des outils et des applications via AppLocker ou un logiciel de restriction d'application tiers. Toutes les applications ou utilitaires administratifs qui ne respectent pas les paramètres sécurisés doivent être mis à niveau ou remplacés par des outils qui respectent les pratiques de développement et d'administration sécurisées. Lorsque des outils nouveaux ou supplémentaires sont nécessaires sur un hôte d'administration, les applications et les utilitaires doivent être soigneusement testés, et si les outils conviennent au déploiement sur des hôtes d'administration, ils peuvent être ajoutés aux systèmes.

Restrictions RDP

- Bien que la configuration spécifique varie en fonction de l'architecture de vos systèmes d'administration, vous devez inclure des restrictions sur les comptes et ordinateurs qui peuvent être utilisés pour établir des connexions RDP (Remote Desktop Protocol) aux systèmes gérés, comme l'utilisation de serveurs de rebond de passerelle Bureau à distance pour contrôler l'accès aux contrôleurs de domaine et à d'autres systèmes gérés à partir d'utilisateurs et de systèmes autorisés.

- Vous devez autoriser les ouvertures de session interactives par les utilisateurs autorisés et supprimer ou même bloquer d'autres types d'ouverture de session qui ne sont pas nécessaires pour l'accès au serveur.

Gestion des correctifs et des configurations

- Les petites organisations peuvent s'appuyer sur des offres telles que Windows Update ou Windows Server Update Services (WSUS) pour gérer le déploiement des mises à jour sur les systèmes Windows, tandis que les grandes organisations peuvent implémenter des logiciels de gestion des correctifs et des configurations destinés aux entreprises, tels que Microsoft Endpoint Configuration Manager. Quels que soient les mécanismes que vous utilisez pour déployer des mises à jour sur votre population générale de serveurs et de stations de travail, vous devez envisager des déploiements distincts pour les systèmes hautement sécurisés tels que les contrôleurs de domaine, les autorités de certification et les hôtes d'administration. En isolant ces systèmes de l'infrastructure de gestion générale, si vos logiciels de gestion ou vos comptes de service sont compromis, la compromission ne s'étend pas facilement aux systèmes les plus sécurisés de votre infrastructure.

- Même si vous ne devez pas implémenter de processus de mise à jour manuelle pour les systèmes sécurisés, vous devez configurer une infrastructure distincte pour la mise à jour des systèmes sécurisés. Même dans les très grandes organisations, cette infrastructure peut généralement être implémentée via des serveurs WSUS dédiés et des objets de stratégie de groupe pour des systèmes sécurisés.

Blocage de l'accès à Internet

- Les hôtes d'administration ne doivent pas être autorisés à accéder à Internet, ni à parcourir l'intranet d'une organisation. Les navigateurs web et les applications similaires ne doivent pas être autorisés sur les hôtes administratifs. Vous pouvez bloquer l'accès Internet pour les hôtes sécurisés via une combinaison de paramètres de pare-feu de périmètre, de configuration WFAS et de configuration de proxy « trou noir » sur des hôtes sécurisés. Vous pouvez également utiliser la liste d'autorisations d'applications pour empêcher l'utilisation de navigateurs web sur des hôtes d'administration.

Virtualisation

- Dans la mesure du possible, envisagez d'implémenter des machines virtuelles en tant qu'hôtes d'administration. À l'aide de la virtualisation, vous pouvez créer des systèmes d'administration par utilisateur qui sont stockés et gérés de manière centralisée, et qui peuvent être facilement arrêtés lorsqu'ils ne sont pas utilisés, en veillant à ce que les informations d'identification ne soient pas laissées actives sur les systèmes d'administration. Vous pouvez également exiger que les hôtes administratifs virtuels soient réinitialisés à un instantané initial après chaque utilisation, ce qui garantit que les machines virtuelles restent intactes. Pour plus d'informations sur les options de virtualisation des hôtes d'administration, consultez la section suivante.

Exemples d'approches pour implémenter des hôtes d'administration sécurisés

- Quelle que soit la façon dont vous concevez et déployez votre infrastructure d'hôte d'administration, vous devez garder à l'esprit les instructions fournies dans « Principes de création d'hôtes d'administration sécurisés » plus haut dans cette rubrique. Chacune des approches décrites ici fournit des informations générales sur la façon dont vous pouvez séparer les systèmes « administratifs » et « de productivité » utilisés par votre service informatique. Les systèmes de productivité sont des ordinateurs que les administrateurs informatiques utilisent pour vérifier la messagerie, naviguer sur Internet et utiliser des logiciels de productivité généraux tels que Microsoft Office. Les systèmes d'administration sont des ordinateurs qui sont renforcés et dédiés à l'utilisation pour l'administration quotidienne d'un environnement informatique.

Exemples d'approches pour implémenter des hôtes d'administration sécurisés

- Le moyen le plus simple d'implémenter des hôtes d'administration sécurisés consiste à fournir à votre personnel informatique des stations de travail sécurisées à partir desquelles ils peuvent effectuer des tâches administratives. Dans une implémentation de stations de travail uniquement, chaque station de travail administrative est utilisée pour lancer des outils de gestion et des connexions RDP afin de gérer les serveurs et d'autres infrastructures. Les implémentations de stations de travail uniquement peuvent être efficaces dans les petites organisations, bien que des infrastructures plus grandes et plus complexes puissent tirer parti d'une conception distribuée pour les hôtes d'administration dans lesquels des serveurs d'administration et des stations de travail dédiés sont utilisés, comme décrit dans « Implémentation de stations de travail d'administration sécurisées et de serveurs de rebond » plus loin dans cette rubrique.

Implémentation de stations de travail physiques distinctes

- Une façon d'implémenter des hôtes d'administration consiste à émettre deux stations de travail pour chaque utilisateur informatique. Une station de travail est utilisée avec un compte d'utilisateur « normal » pour effectuer des activités telles que la vérification de la messagerie et l'utilisation d'applications de productivité, tandis que la deuxième station de travail est strictement dédiée aux fonctions administratives.

- Pour la station de travail de productivité, le personnel informatique peut recevoir des comptes utilisateur normaux plutôt que d'utiliser des comptes privilégiés pour se connecter à des ordinateurs non sécurisés. La station de travail administrative doit être configurée avec une configuration strictement contrôlée et le personnel informatique doit utiliser un autre compte pour se connecter à la station de travail administrative.

Implémentation de stations de travail physiques distinctes

- Si vous avez implémenté des cartes à puce, les stations de travail administratives doivent être configurées pour exiger des ouvertures de session par carte à puce, et le personnel informatique doit disposer de comptes distincts pour une utilisation administrative, également configurés pour exiger des cartes à puce à l'ouverture de sessions interactives. L'hôte d'administration doit être renforcé comme décrit précédemment, et seuls les utilisateurs informatiques désignés doivent être autorisés à se connecter localement à la station de travail d'administration.

Avantages

- En implémentant des systèmes physiques distincts, vous pouvez vous assurer que chaque ordinateur est configuré de manière appropriée pour son rôle et que les utilisateurs informatiques ne peuvent pas exposer par inadvertance des systèmes administratifs à des risques.

Inconvénients

- L'implémentation d'ordinateurs physiques distincts augmente les coûts matériels.
- La connexion à un ordinateur physique avec des informations d'identification utilisées pour administrer les systèmes distants met en mémoire cache les informations d'identification.
- Si les stations de travail d'administration ne sont pas stockées de manière sécurisée, elles peuvent être vulnérables à la compromission via des mécanismes tels que des enregistreurs de clés matérielles physiques ou d'autres attaques physiques.

Implémentation d'une station de travail physique sécurisée avec une station de travail de productivité virtualisée

- Dans cette approche, les utilisateurs informatiques disposent d'une station de travail d'administration sécurisée à partir de laquelle ils peuvent effectuer des fonctions d'administration quotidiennes, à l'aide des outils d'administration de serveur distant (RSAT) ou des connexions RDP aux serveurs dans leur domaine de responsabilité. Lorsque les utilisateurs informatiques doivent effectuer des tâches de productivité, ils peuvent se connecter via RDP à une station de travail de productivité distante s'exécutant en tant que machine virtuelle. Des informations d'identification distinctes doivent être utilisées pour chaque station de travail, et des contrôles tels que les cartes à puce doivent être implémentés.

Avantages

- Les stations de travail administratives et les stations de travail de productivité sont séparées.
- Le personnel informatique utilisant des stations de travail sécurisées pour se connecter à des stations de travail de productivité peut utiliser des informations d'identification et des cartes à puce distinctes, et les informations d'identification privilégiées ne sont pas déposées sur l'ordinateur moins sécurisé.

Inconvénients

- L'implémentation de la solution nécessite un travail de conception et d'implémentation et des options de virtualisation robustes.
- Si les stations de travail physiques ne sont pas stockées en toute sécurité, elles peuvent être vulnérables aux attaques physiques qui compromettent le matériel ou le système d'exploitation et les rendent vulnérables à l'interception des communications.

Implémentation d'une station de travail sécurisée unique avec des connexions pour séparer les Machines Virtuelles « de productivité » et « administratives »

- Dans cette approche, vous pouvez fournir aux utilisateurs informatiques une seule station de travail physique verrouillée comme décrit précédemment, sur laquelle ils n'ont pas d'accès privilégié. Vous pouvez fournir des connexions de services Bureau à distance aux machines virtuelles hébergées sur des serveurs dédiés, en fournissant au personnel informatique une machine virtuelle qui exécute la messagerie et d'autres applications de productivité, et une deuxième machine virtuelle configurée en tant qu'hôte d'administration dédié de l'utilisateur.

- Vous devez exiger une carte à puce ou une autre ouverture de session multifacteur pour les machines virtuelles, en utilisant des comptes distincts autres que le compte utilisé pour vous connecter à l'ordinateur physique. Une fois qu'un utilisateur informatique se connecte à un ordinateur physique, il peut utiliser sa carte à puce de productivité pour se connecter à son ordinateur de productivité distant et un compte et une carte à puce distincts pour se connecter à son ordinateur d'administration distant.

Avantages

- Les utilisateurs informatiques peuvent utiliser une seule station de travail physique.
- En exigeant des comptes distincts pour les hôtes virtuels et en utilisant les connexions des services Bureau à distance aux machines virtuelles, les informations d'identification des utilisateurs informatiques ne sont pas mises en mémoire cache sur l'ordinateur local.
- L'hôte physique peut être sécurisé au même degré que les hôtes d'administration, ce qui réduit la probabilité de compromission de l'ordinateur local.
- Dans les cas où la productivité de la machine virtuelle d'un utilisateur informatique ou sa machine virtuelle d'administration peut avoir été compromise, la machine virtuelle peut facilement être réinitialisée à un état « réputé bon ».
- Si l'ordinateur physique est compromis, aucune information d'identification privilégiée n'est mise en mémoire cache, et l'utilisation de cartes à puce peut empêcher la compromission des informations d'identification par les enregistreurs de frappe.

Inconvénients

- L'implémentation de la solution nécessite un travail de conception et d'implémentation et des options de virtualisation robustes.
- Si les stations de travail physiques ne sont pas stockées en toute sécurité, elles peuvent être vulnérables aux attaques physiques qui compromettent le matériel ou le système d'exploitation et les rendent vulnérables à l'interception des communications.

Implémentation de stations de travail d'administration sécurisées et de serveurs de rebond

- En guise d'alternative à la sécurisation des stations de travail d'administration, ou en combinaison avec celles-ci, vous pouvez implémenter des serveurs de rebond sécurisés, et les utilisateurs administratifs peuvent se connecter aux serveurs de rebond à l'aide de RDP et de cartes à puce pour effectuer des tâches d'administration.

- Les serveurs de rebond doivent être configurés pour exécuter le rôle Passerelle des services Bureau à distance afin de vous permettre d'implémenter des restrictions sur les connexions au serveur de rebond et aux serveurs de destination qui seront gérés à partir de celui-ci. Si possible, vous devez également installer le rôle Hyper-V et créer des bureaux virtuels personnels ou d'autres machines virtuelles par utilisateur que les utilisateurs administratifs peuvent utiliser pour leurs tâches sur les serveurs de rebond.

Implémentation de stations de travail d'administration sécurisées et de serveurs de rebond

- En donnant aux utilisateurs administratifs des machines virtuelles par utilisateur sur le serveur de rebond, vous fournissez une sécurité physique pour les stations de travail d'administration, et les utilisateurs administratifs peuvent réinitialiser ou arrêter leurs machines virtuelles lorsqu'elles ne sont pas utilisées. Si vous préférez ne pas installer le rôle Hyper-V et le rôle Passerelle des services Bureau à distance sur le même hôte d'administration, vous pouvez les installer sur des ordinateurs distincts.

- Dans la mesure du possible, les outils d'administration à distance doivent être utilisés pour gérer les serveurs. La fonctionnalité Outils d'administration de serveur distant (RSAT) doit être installée sur les machines virtuelles des utilisateurs (ou sur le serveur de rebond si vous n'implémentez pas les machines virtuelles par utilisateur pour l'administration), et le personnel administratif doit se connecter via RDP aux machines virtuelles pour effectuer des tâches administratives.

Implémentation de stations de travail d'administration sécurisées et de serveurs de rebond

- Dans les cas où un utilisateur administratif doit se connecter via RDP à un serveur de destination pour le gérer directement, la passerelle des services Bureau à distance doit être configurée pour autoriser la connexion uniquement si l'utilisateur et l'ordinateur appropriés sont utilisés pour établir la connexion au serveur de destination. L'exécution d'outils RSAT (ou similaires) doit être interdite sur les systèmes qui ne sont pas des systèmes de gestion désignés, tels que les stations de travail à usage général et les serveurs membres qui ne sont pas des serveurs de rebond.

Avantages

- La création de serveurs de rebond vous permet de mapper des serveurs spécifiques à des « zones » (collections de systèmes ayant des exigences de configuration, de connexion et de sécurité similaires) dans votre réseau et d'exiger que l'administration de chaque zone soit effectuée par le personnel administratif qui se connecte à partir d'hôtes d'administration sécurisés vers un serveur de « zone » désigné.

- En mappant des serveurs de rebond à des zones, vous pouvez implémenter des contrôles granulaires pour les propriétés de connexion et les exigences de configuration, et identifier facilement les tentatives de connexion à partir de systèmes non autorisés.

- En implémentant des machines virtuelles par administrateur sur des serveurs de rebond, vous faites appliquer l'arrêt et la réinitialisation des machines virtuelles à un état réputé bon lorsque les tâches d'administration sont terminées. En faisant appliquer l'arrêt (ou le redémarrage) des machines virtuelles lorsque les tâches d'administration sont terminées, les machines virtuelles ne peuvent pas être ciblées par des attaquants, et les attaques par vol d'informations d'identification ne sont pas réalisables, car les informations d'identification mises en mémoire cache ne sont pas conservées après un redémarrage.

Inconvénients

- Des serveurs dédiés sont requis pour les serveurs de rebond, qu'ils soient physiques ou virtuels.
- L'implémentation de serveurs de rebond et de stations de travail d'administration dédiés nécessite une planification et une configuration minutieuses qui correspondent à toutes les zones de sécurité configurées dans l'environnement.

Merci Pour Votre Attention !