Maîtriser les comptes à privilèges

Dr. Götz Güttich

Les comptes à privilèges comme ceux des administrateurs présentent des risques liés à la sécurité. Les comptes des fournisseurs de service (qui accèdent à distance aux systèmes d'une entreprise) posent aussi des problèmes dans la pratique. Des personnes malveillantes peuvent pirater ces comptes et utiliser les droits associés pour accéder aux données de l'organisation à laquelle elles appartiennent. En raison du nombre croissant de tentatives de piratage ciblées, cette menace gagne de plus en plus en importance. En plus des hautes exigences de la compliance, les risques d'attaques augmentent en raison de l'utilisation croissante d'applications hébergées en externe ainsi que des services cloud. Les solutions pour la gestion d'accès à privilèges se chargent de cette problématique. Nous avons regardé ce qu'ADMINBASTION Suite de WALLIX peut accomplir dans ce contexte.

ADMINBASTION Suite (WAB Suite) de WALLIX est une solution permettant une telle sécurisation des comptes à privilèges (Privileged Account Management, PAM). Elle assure la gestion des mots de passe, sécurise l'accès aux données et systèmes importants et surveille en temps réel les activités effectuées via les comptes à privilèges. Peu importe s'il s'agit d'utilisateurs externes ou travaillant en interne. Concrètement, WAB Suite englobe trois produits-clés : le Password Manager, le Session Manager et l'Access Manager. En cours d'utilisation, ces trois produits veillent à ce que les bons utilisateurs puissent, au bon moment, accéder aux bonnes ressources.

Le WAB Password Manager enregistre les données d'accès pour les comptes administrateurs, les comptes locaux et les comptes administrateurs des bases de données dans un coffre-fort central certifié ANSSI en France et FSTEK en Russie.

L'ANSSI coopère étroitement avec les autorités allemandes dans le domaine de la cybersécurité et est le pendant français du BSI allemand (office fédéral allemand pour la sécurité en matière de technologies de l'information). Dans ce coffre-fort, les données peuvent être gérées via une seule console. Il est également possible de créer, cacher, afficher ou modifier ces données. Pendant leur travail, les utilisateurs finaux ne peuvent pas voir les mots de passe. Il est ainsi possible d'utiliser automatiquement des mots de passes longs, complexes et aléatoires.

Le WAB Session Manager gère et surveille tous les accès des utilisateurs à privilèges à des appareils et applications dans le réseau et as-

sure en même temps les audits. Le monitoring – et ainsi aussi l'alerting – sont effectués en temps réel. Chaque accès est toujours attribué à une identité unique ce qui permet de rapporter à chaque utilisateur la responsabilité de ses actions.

Enfin, le WAB Access Manager est un portail web via lequel les utilisateurs peuvent accéder à toute ressource dont ils ont besoin. La sécurisation des comptes à privilèges fonctionne même sur plusieurs sites, clients ou réseaux. C'est pour cela que ce produit peut aussi bien être utilisé par des fournisseurs de cloud que par des utilisateurs finaux. En cours d'utilisation, l'accès aux systèmes souhaités s'effectue en un seul clic.

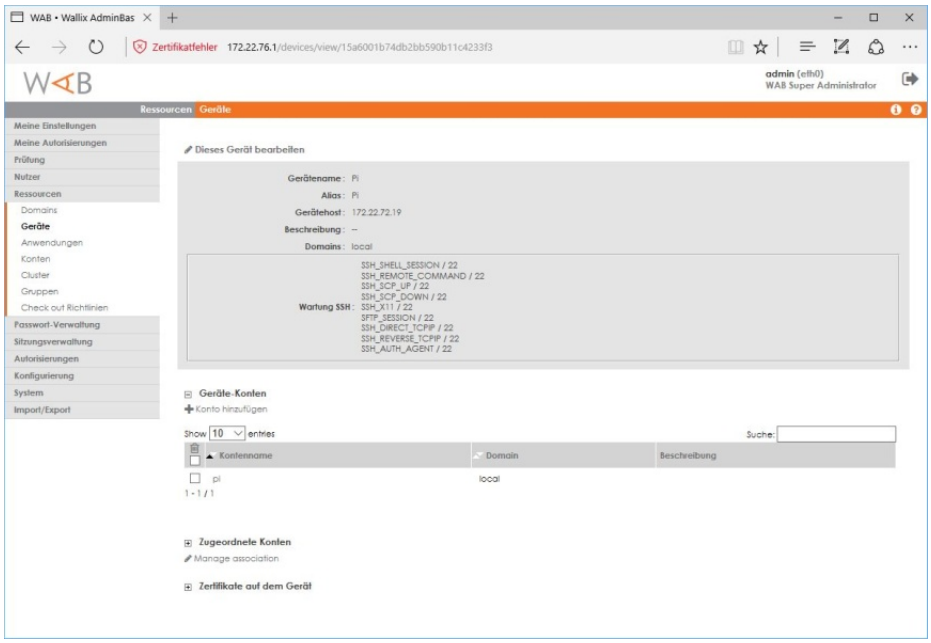
Le test

Pour le test, WALLIX a mis à notre disposition une appliance sur laquelle la WAB Suite a déjà été installée. Nous avons intégré cette appliance dans notre environnement, nous sommes familiarisés avec l'étendue de cette solution et avons géré des comptes utilisateurs à privilèges dans notre réseau. En plus, nous avons enregistré plusieurs sessions lors de l'utilisation de ces comptes et avons testé les fonctions de monitoring.

Mise en service

Pour la mise en service de ce produit, il suffit d'intégrer l'appliance ou l'appliance virtuelle (le produit est aussi disponible sous cette forme) dans le réseau et de la démarrer. Ensuite, nous nous sommes connectés à la console locale du Debian-Linux utilisé comme système d'exploitation par l'appliance WALLIX, et avons adapté la configuration réseau du système à notre environnement.

Dès que ce paramétrage a été réalisé, nous avons pu nous



Le compte d'appareil pour l'accès SSH sur un Raspberry-Pi via Linux

connecter via la nouvelle adresse IP avec l'outil de configuration de la solution. Après le log-in, l'outil de configuration nous a directement demandé de modifier le mot de passe mis par défaut (admin) du compte administrateur.

Cela est raisonnable pour assurer qu'aucun produit avec un mot de passe mis par défaut ne passe en mode productif. Après avoir modifié le mot de passe, nous avons pu commencer le travail pratique.

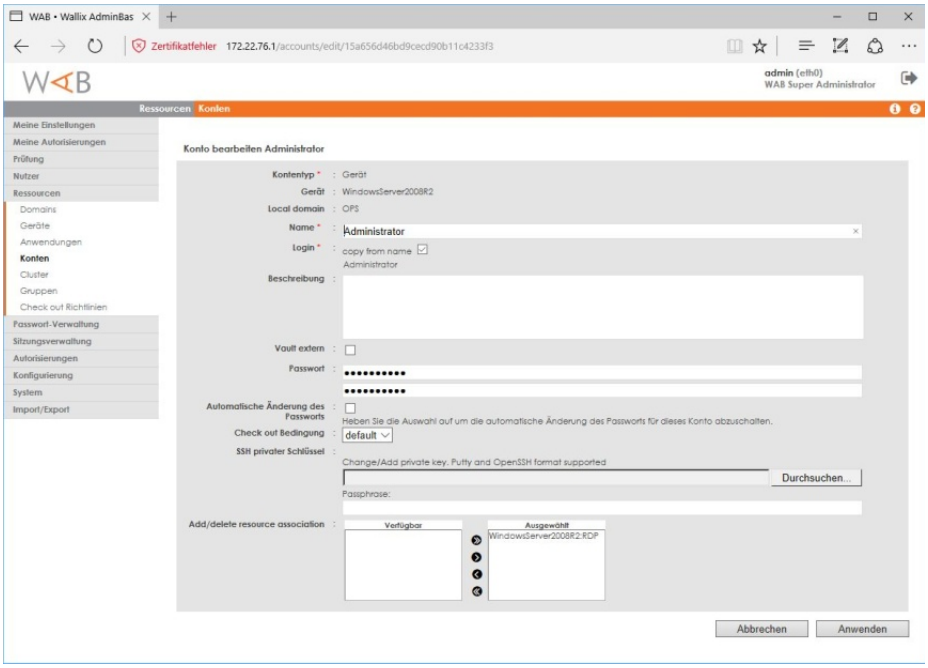
En cours d'utilisation, l'appliance fait office de proxy virtuel, c'est-à-dire que les utilisateurs accèdent à la solution de WALLIX puis celle-ci établit alors une connexion au système cible souhaité. C'est la raison pour laquelle ce produit est aussi bien approprié pour des prestataires de services que pour des administrateurs internes de PME.

La configuration des postes cibles individuels ne doit pas nécessairement être modifiée si bien que les log-in directs fonctionnent aussi. Comme nous l'avons mentionné, il y a aussi la possibilité d'automatiser la gestion des mots de passe et de la confier complètement à WAB Suite. Dans ce cas, tous les accès passent par la solution WALLIX. Nous reviendrons en détails sur ce sujet plus tard.

Lors du test, nous avons d'abord regardé l'étendue de cet outil de gestion. La solution dispose d'un menu sur le côté gauche via lequel toutes les fonctions du produit de WALLIX sont accessibles.

Pendant que nous nous familiarisions avec les différentes sections du menu, la connexi-

on à l'appliance s'est brusquement interrompue. Après que nous nous soyons reconnectés à la console locale du serveur, nous avons remarqué que la solution avait réinitialisé son ancienne configuration qui se trouvait dans un autre sous-réseau que notre environnement de test.



Un compte administrateur Windows pour accès RDP

Pour cette raison, nous avons refait la configuration du réseau, rétabli la connexion à l'interface web et réadapté les paramètres réseau. Ensuite, la connexion réseau est restée stable.

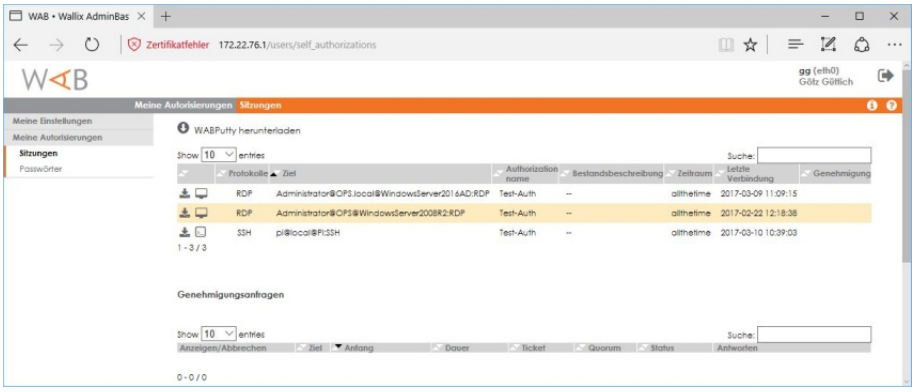
La connexion avec un serveur Windows

Une fois que le tout fonctionnait bien, nous avons commencé à établir deux connexions, l'un à un système Debian-Linux et l'autre à un poste sous Windows Server 2016. Le but était d'accéder au Windows Server via RDP et au poste Linux via SSH. Pour établir la connexion RDP, nous sommes allés à « Utilisateurs/Comptes » et avons créé un compte utilisateur avec des droits d'utilisation normaux sur l'appliance. Via ce compte, les utilisateurs se sont plus tard connectés avec le système de WALLIX pour accéder ainsi aux postes pour lesquels ils avaient une autorisation.

Ensuite, nous avons créé un groupe auquel nous avons attribué nos comptes utilisateurs locaux. A l'aide de ces groupes, il est possible d'attribuer différents droits à différents utilisateurs dans le réseau – par exemple aux collaborateurs du département informatique ou à des utilisateurs externes.

Ensuite, nous sommes allés à « Ressources/Appareils » pour y créer un nouvel appareil. Nous l'avons nommé « Windows2016AD » car il s'agissait d'un contrôleur Active Directory. De plus, nous avons saisi l'adresse IP et le domaine.

Ensuite, nous avons sélectionné le protocole RDP correspondant. En plus de RDP et SSH, le système soutient également Telnet, RLOGIN et VNC. Lors de la configuration des protocoles, les collaborateurs responsables sont, si nécessaire, en position de saisir les ports utilisés ainsi que d'autres informations. Une fois l'appareil créé, nous



Après le log-in en tant qu'utilisateur, une liste des systèmes client autorisés est affichée

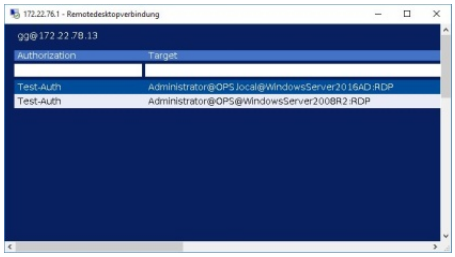
Celui-ci a été utilisé pour réaliser le log-in sur l'appareil terminal. Vu que notre objectif était de sécuriser nos comptes à privilèges à l'aide de la solution de WALLIX, nous avons pu aller à « Ressources/Comptes » pour y créer un compte utilisateur pour ce nouvel appareil.

ons utilisé, dans ce but, le compte administrateur du serveur Windows.

Ici, il est également possible d'enregistrer, en plus des mots de passe, des clés privées, par exemple pour des comptes SSH, ou bien des passphrases. Une fois que nous avons saisi le mot de passe et la description de notre compte, nous l'avons directement attribué à notre appareil.

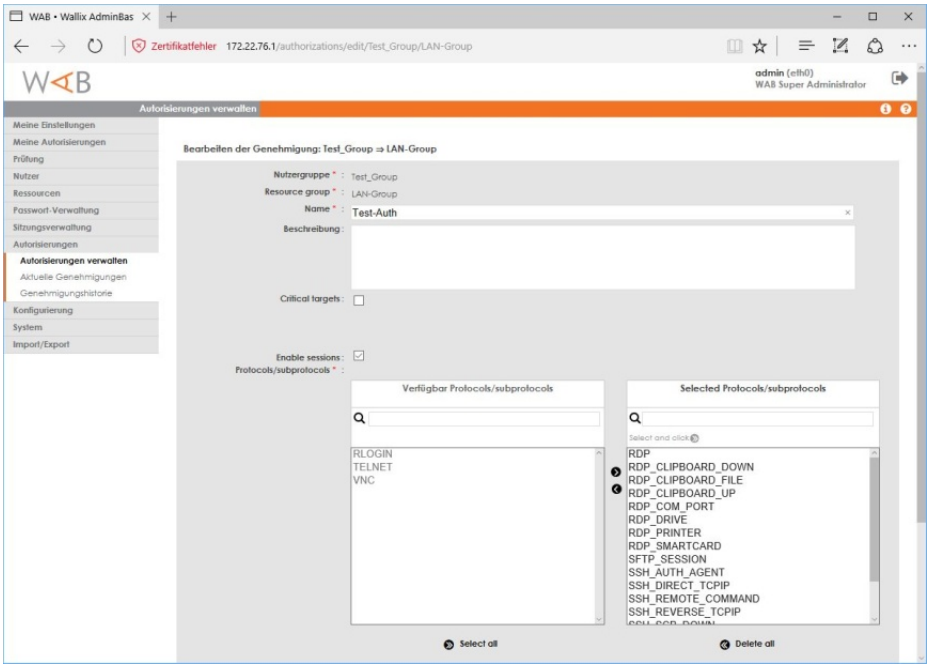
Dans le cadre de la configuration des comptes de l'appareil, il y a également l'option d'activer la modification automatique du mot de passe que nous avons déjà mentionnée. Cette fonction permet de confier la gestion des mots de passe pour les comptes à privilèges (ou pour tous les comptes, mais cela a plus de sens pour les comptes à privilèges) complètement à la solution de WALLIX.

Pour ce faire, il fallait seulement configurer le niveau des



Si on accède à WAB Suite via RDP, une liste des clients RDP autorisés pour ce compte sera affichée

mots de passe et activer la modification automatique des mots de passe. Ensuite, AdminBastion crée régulièrement des nouveaux mots de passe pour les comptes en question. La période de modification souhaitée peut être définie. La solution les enregistre dans son coffre-fort et les active sur les systèmes cibles en question.



Pour notre groupe de test, nous avons autorisé les protocoles RDP et SSH

Dans ce cas, les mots de passe ne sont plus connus aux utilisateurs et ces derniers peuvent uniquement accéder à leurs postes via la solution de WALLIX. Une fois que le compte d'appareil a été défini, nous avons créé un nouveau groupe sous « Ressources/Groupes » et lui avons attribué le nouveau compte pour qu'il puisse être utilisé par les utilisateurs.

Enfin, nous avons encore testé la fonction « Autorisations/Gérer les autorisations », créé un groupe et autorisé le protocole RDP pour celui-ci. En même temps, nous avons activé l'enregistrement des sessions qui est l'un des points forts du produit de WALLIX. Nous verrons les détails plus tard. Voilà, la première connexion était prête.

Le premier accès

Pour utiliser cette nouvelle connexion, nous avons connecté notre compte utilisateur que nous avions créé auparavant, avec l'appliance et sommes arrivés sur une interface web affichant deux points de menu. Le premier point s'appelle « Mes préférences » et permet de sélectionner la langue que l'on souhaite utiliser pour les comptes et de saisir l'adresse e-mail des utilisateurs. En plus, il est possible d'y enregistrer des clés SSH et GPG.

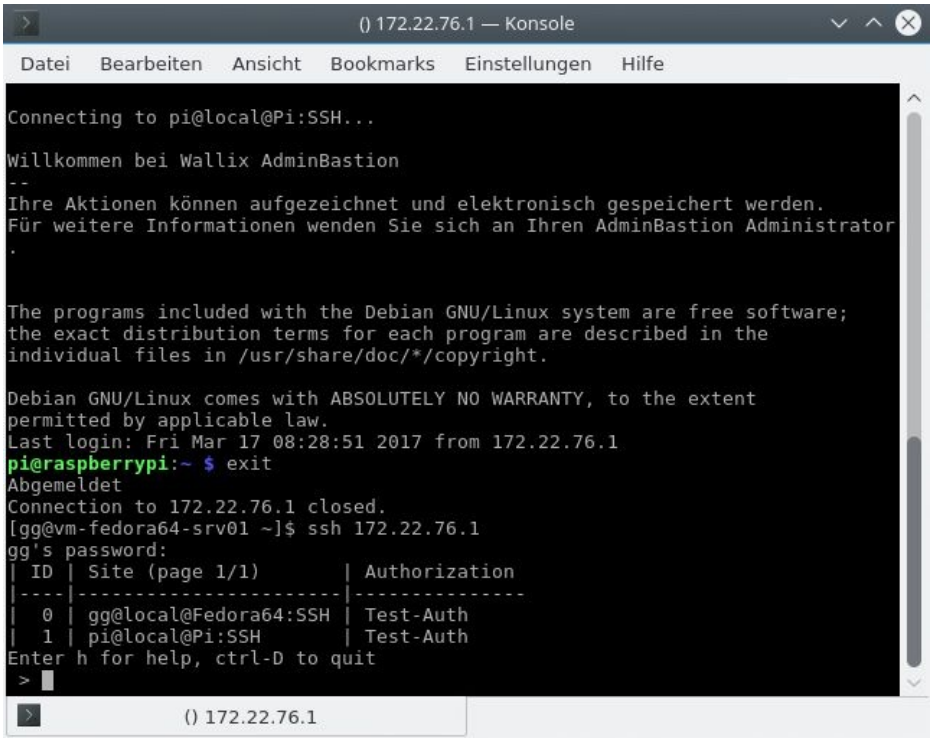
Le menu « Mes autorisations » nous intéresse plus. Ici, nous trouvons une liste affichant tous les systèmes auxquels le compte utilisateur correspondant peut accéder. A ce moment-là, nous n'avons logiquement vu que le serveur Windows.

En plus du nom du système, cette liste englobe aussi des informations concernant le protocole utilisé ou la dernière

connexion. De plus, il met à notre disposition deux icônes pour le système cible. L'une des icônes permet le téléchargement d'un fichier de configuration RDP via lequel une connexion peut être établie en un seul clic. Cependant, si un utilisateur souhaite se connecter via cette fonction, il devra toujours saisir son mot de passe pour établir la connexion.

En alternative, les responsables peuvent établir une connexion directe via la deuxième icône. Pour ce faire, aucun mot de passe n'est nécessaire. Cependant, cette connexion ne dure que 30 secondes et est automatiquement interrompue après ce laps de temps. Pendant notre test, les deux modes de fonctions fonctionnaient directement.

D'ailleurs, les accès via RDP ne sont pas seulement possibles via l'interface web. Il y a aussi la possibilité de se connecter directement avec l'appliance via un client RDP. La solution de WALLIX affiche alors dans une liste les systèmes cibles RDP auxquels le compte en question peut accéder et établit la connexion en appuyant sur une touche. Si besoin, WAB Suite permet aussi de rendre disponible dans le réseau des applications individuelles via RDP à l'aide d'un serveur de rebond Windows avec des rôles de services de terminaux ou de bureaux à distance installés.

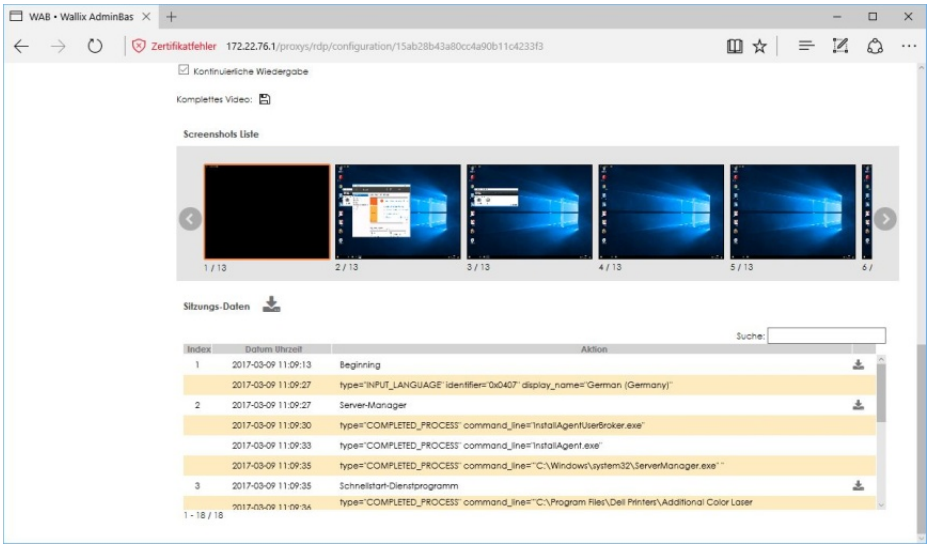


Après le log-in SSH à l'appliance à partir de Linux, le système affiche une liste des systèmes SSH autorisés et permet ainsi l'établissement de la connexion

Ensuite, nous avons configuré l'accès SSH sur notre serveur Debian mentionné plus haut. Cette configuration ressemble à celle faite pour le RDP. D'abord, nous avons créé l'appareil et saisi l'adresse IP et le nom. Par contre, nous avons activé le protocole SSH au lieu du RDP.

Ensuite, il fallait définir le mot de passe et d'autres informations du compte d'appareil. Ici, nous avons utilisé le compte root du serveur et désactivé la modification automatique du mot de passe.

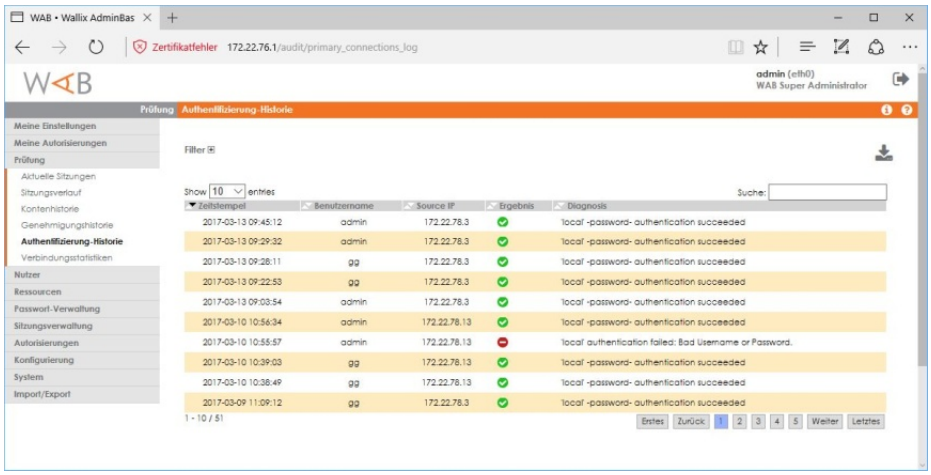
Après avoir ajouté le nouveau compte à l'appareil Debian et au groupe, nous avons encore sélectionné le protocole SSH dans les autorisations. Et voilà, la connexion était disponible.



Une session RDP enregistrée

Accès SSH en tant qu'utilisateur

Dans la pratique, l'accès SSH diffère de celui en RDP. Certes, les utilisateurs peuvent sélectionner le système cible SSH via la liste de leurs autorisations mais l'établissement de la connexion sous Windows ne peut être réalisée qu'avec une version spéciale du client putty. Celle-ci s'appelle WABputty et peut être téléchargée directement dans l'interface utilisateur de l'appliance. Une fois qu'elle a été installée sur le poste client utilisé, les accès SSH fonctionnent avec succès. Sinon, les utilisateurs peuvent aussi se connecter via SSH à l'appliance WALLIX. Cela fonctionne aussi bien à partir de Linux qu'avec putty sous Windows. Un peu comme lors des accès avec le client RDP, l'appliance présente aux utilisateurs une liste dans laquelle figurent les systèmes cibles disponibles puis elle établit une connexion après la sélection d'une entrée.



Des statistiques détaillées : l'historique des log-in et des tentatives de log-in permet de surveiller toutes les activités

La suite du test

Dans la suite du test, nous nous sommes familiarisés en détail avec les fonctions de la solution de WALLIX. Nous avons utilisé l'enregistrement des sessions et ajouté à notre environnement d'autres systèmes cibles, par exemple sous Windows Server 2008 R2 et Fedora Linux. Il ne rentre pas dans le cadre du présent test de détailler chaque fonction de la solution.

Cependant, il est judicieux de mentionner encore une fois la fonction d'enregistrement du produit. Si un utilisateur autorisé se connecte à l'appliance, il aura la possibilité d'aller dans la zone « Vérification » pour y consulter une liste des sessions actuelles et l'historique des sessions passées.

Il existe également l'option d'analyser en détail l'historique de chaque session une fois que cette fonction a été activée. Dans le cas des sessions SSH, l'historique est disponible sous forme de fichiers texte et ttyrec.

Dans ce contexte, nous souhaitons surtout souligner le soutien de ttyrec. Grâce à cet outil, il est non seulement possible de lire ses propres commandes mais également de les faire afficher en temps réel sur une console pour que l'administrateur puisse à tout moment voir ce qui s'est passé et quand. Pour les connexions RDP, WABSuite crée des vidéos Flash qui peuvent être consultées et téléchargées directement dans l'interface web. En plus, la solution met à notre disposition des copies d'écran qui sont générées à base des actions détectées. Ici aussi, on sait toujours quelle action a été réalisée quand, ce qui facilite les audits et assure la compliance. L'offre de l'appliance est complétée par les statistiques détaillées relatives aux connexions qui affichent par exemple le nombre de connexions WAB par utilisateur ou la connexion cible selon la durée ou selon la date.

Notre bilan

En phase de test, ADMINBASTION Suite de WALLIX nous a fait une très bonne impression. Le produit ne permet non seulement un accès facile et sécurisé aux comptes à privilèges des composants du réseau mais s'occupe également de la gestion des mots de passe et met à disposition des applications dans le réseau si besoin. La WAB Suite est complétée par les fonctions détaillées relatives à l'auditing qui vous montrent qui a fait quoi et quand.

Dr Götz Güttich est le rédacteur en chef de Sysbus.eu. En outre, il dirige l'Institut pour l'analyse des composants IT (Institut zur Analyse von IT-Komponenten, IAIT).