HAFS
Distributeur à valeur ajoutée

Distributeur à valeur ajoutée de solutions IT

Cybersécurité | Réseaux | Wi-Fi | Stockage

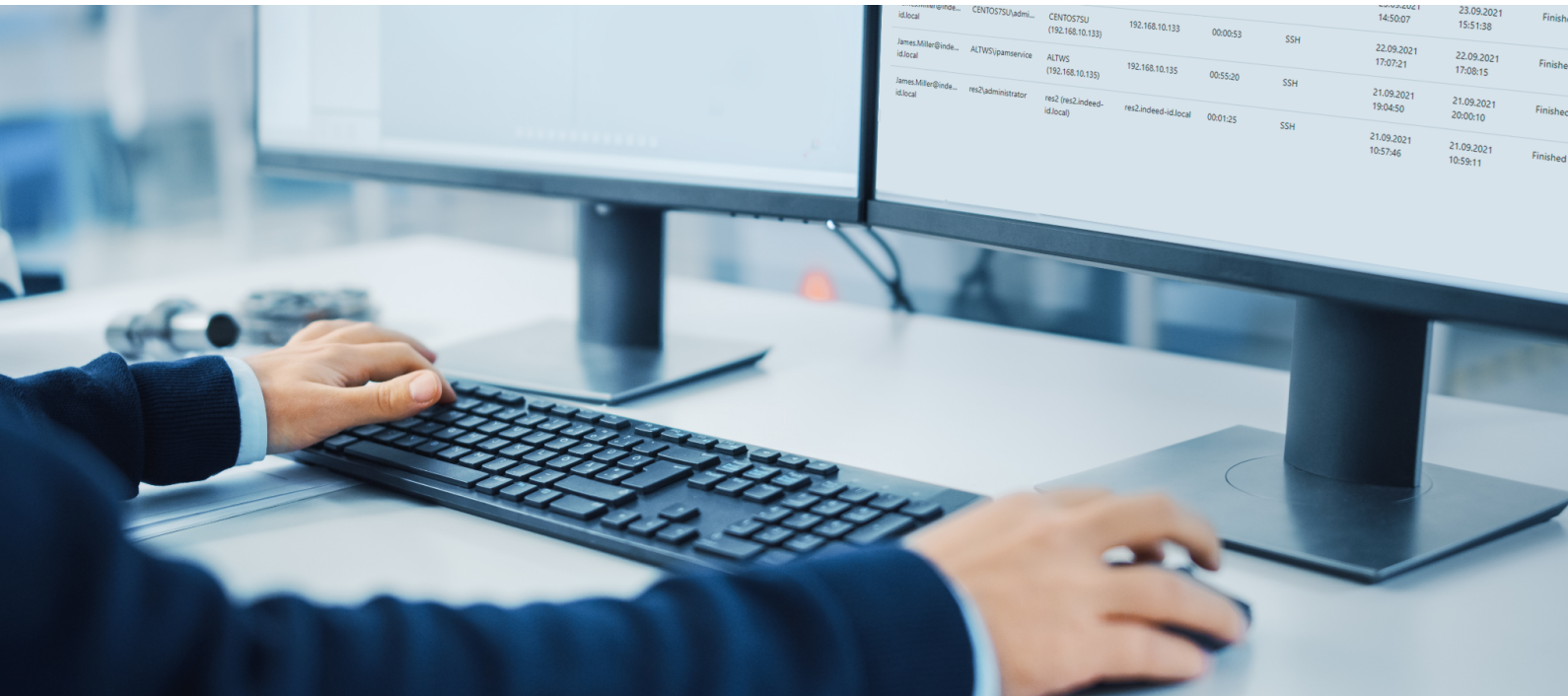
Une solution pour chaque environnement

Axidian

WHITE PAPER

Axidian Privilege

Contrôle de l'accès des utilisateurs à privilèges aux systèmes informatiques de la société



Contenu

Accès à privilèges - une menace pour la sécurité

L'augmentation constante et la complexité de l'infrastructure IT des sociétés font la gestion de l'accès à privilèges l'une des tâches les plus importantes de la sécurité de l'information. Le nombre croissant des systèmes d'information et de la diversité des scénarios d'accès empêchent la realisation de cette tâche. Ayant reçu les données du compte administratif (CA), le malfaiteur peut causer des dommages beaucoup plus graves à l'entreprise que dans le cas de la compromission des informations d'identification d'un employé ordinaire. Les comptes administratifs peuvent être utilisés pour désactiver la protection, arrêter les systèmes d'information et accéder à des informations confidentielles. Il est plus difficile de protéger l'accès à privilèges, il est impossible de résoudre ce problème en utilisant des approches communes de protection des comptes administratifs, cela nécessite des solutions spécialisées.

Utilisateurs à privilèges

Avoir des droits accrus d'accès à des informations importantes et à des fonctions essentielles du logiciel et du matériel peuvent les catégories différentes de personnel de bureau et ceux qui travaillent à l'extérieur de la société.

Administrateurs de systèmes d'information

Chaque appareil et chaque logiciel d'application ou celui de système ont leurs propres comptes administratifs. C'est le groupe le plus évident d'employés à privilèges, comme par exemple:

- Administrateurs Directeurs Actifs
- Administrateurs de l'équipement de réseau
- Administrateurs de bases de données
- Administrateurs de serveurs (Windows, Unix/Linux)
- Administrateurs VDI

Utilisateurs d'affaires

Bien que les utilisateurs d'affaires n'aient pas d'accès administratif, ils peuvent avoir de grands pouvoirs dans le cadre des systèmes d'information particuliers. Par exemple, ils peuvent avoir la possibilité d'effectuer des transferts monétaires, de gérer le processus de production et d'accéder à des données qui représentent un secret commercial.

Maîtres d'œuvre et partenaires

Les employés des maître d'œuvre font généralement l'accompagnement de logiciels et de matériel spécialisés. Ils peuvent être vendeurs ou intégrateurs. En général, ces utilisateurs ont accès à distance à l'infrastructure de l'entreprise ce qui complique plus le contrôle de leur fonctionnement.

Comptes de service administratifs

Les comptes de service administratifs sont utilisés pour automatiser les processus. Les divers services et démons, scripts et d'autres logiciels fonctionnent en leur nom. Ces comptes administratifs sont faciles à oublier, car les employés ne les utilisent pas explicitement tous les jours. Cela crée des difficultés et des risques supplémentaires.

Gestion d’ accès à privilèges

Pour résoudre avec succès le problème de gestion et de la protection des accès à privilèges, vous devez vous assurer que les tâches suivantes sont accomplies:

- Gestion centralisée de l'accès des employés aux ressources contrôlées.
- Empêchement, detection et contrôle de l'utilisation incontrôlée des comptes à privilèges . Le stockage des mots de passe secrets, vérification régulière et remplacement des mots de passe par des valeurs aléatoires.
- Réduction du nombre de comptes à privilèges requis pour gérer les systèmes d'information de l'entreprise. Enregistrement dans le journal d'accès des tentatives d'utilisation de comptes à privilèges, en indiquant quel employé, quand et à quel compte administratif a eu l’accès.
- Assurance de l'authentification multifactorielle des employés lorsque vous accédez à des comptes à privilèges.
- Mise en œuvre des mécanismes d'enquête sur les incidents et de reconstitution des faits.

Le logiciel Indeed Gestion de l’accès à privilèges (Axidian Privilège) est un système de gestion d'accès pendant l’utilisation des comptes administratifs à privilèges. La façon dont Axidian PAM résout les tâches énumérées est décrite ci-dessous.

Gestion d'accès centralisé

Axidian PAM stocke des informations sur tous les comptes administratifs à privilèges et les autorisations d'utilisation délivrées. Les autorisations dans Axidian PAM sont le principal mécanisme permettant d'accorder un accès à privilèges aux employés. L'autorisation définit les options d'accès suivantes :

- qui a l’accès - quels utilisateurs ou groupes d'utilisateurs;
- où - quels serveurs, matériel et applications seront disponibles pour fonctionner;
- avec quels droits - quel compte administratif sera utilisé pour se connecter;
- dans quelles conditions l'accès est accordé - pour combien de temps et avec quel emploi du temps, selon quels protocoles.

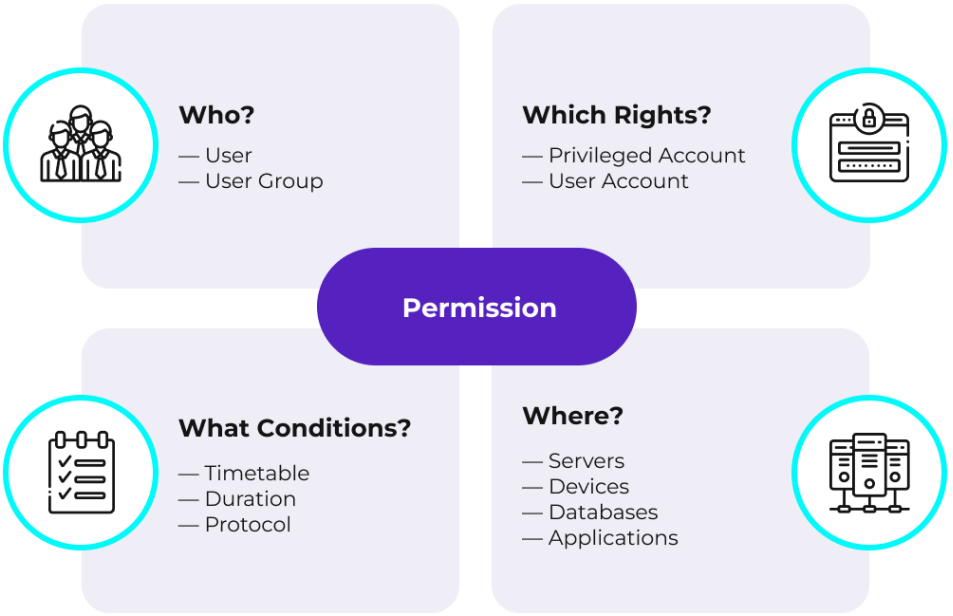


Figure 1. Paramètres d'autorisation d'accès

Les autorisations sont délivrées d'une façon centralisée par l'administrateur dans la console de gestion Axidian PAM. L'autorisation peut être suspendue pour résilier temporairement l'accès ou révoquée si l'accès n'est plus nécessaire. Axidian PAM prend en charge l'intégration avec les systèmes de classe Service/Help Desk. Cette intégration permet d'utiliser le processus de l'accordement de l'accès dans le système habituel des employés et de délivrer et de retirer automatiquement des autorisations dans Indeed PAM dans le cadre de ce processus de travail. À cette fin, Axidian PAM propose deux mécanismes de communication: l'utilitaire de ligne de commande et API.

Le mécanisme d'autorisation complète un autre outil de contrôle d'accès, les stratégies Axidian PAM. Les stratégies définissent des paramètres d'accès communs tels que:

- les commandes autorisées et interdites dans les sessions ssh
- si l'administrateur PAM doit approuver l'ouverture d'une session à privilèges
- les ressources locales disponibles du PC d'utilisateur à la ressource distante (disques, presse-papiers, etc.)
- la nécessité de réinitialiser le mot de passe du compte administratif à privilèges
- après la session à privilèges
- l'utilisation exclusive d'un compte à privilèges (impossibilité d'ouvrir deux sessions sous
- le même compte)
- la durée maximale de la session

Contrôle de l'utilisation des comptes à privilèges

Pour contrôler l'utilisation des comptes I à privilèges Axidian PAM met en œuvre quatre mécanismes:

- Découverte des comptes à privilèges
- Stockage des informations d'identification
- Rotation des mots de passe et des clés SSH
- Utilisation sécurisée des informations d'identification

Détection de comptes administratifs

Axidian PAM comprend le moteur Account Discovery qui met en œuvre des fonctions de recherche régulière de nouveaux comptes administratifs sur les ressources et domaines connectés. La fréquence de recherche est réglable et peut varier selon les groupes de ressources. Lorsque le système trouve un nouveau compte qui n'est pas encore enregistré dans PAM, les informations le concernant sont enregistrées dans un référentiel commun. En outre, un événement approprié est enregistré dans le journal, auquel l'administrateur peut recevoir une notification par courrier afin de décider plus rapidement d'utiliser le nouveau compte administratif. Axidian PAM prend en charge la recherche de comptes administratifs sur les types de ressources suivants:

- PC Windows et serveurs
- systèmes * nix
- Système de gestion des bases de données (MS SQL, MySQL, PostgreSQL, Oracle DB)
- Active Directory

Stockage des informations d'identification

Axidian PAM est un référentiel centralisé d'informations d'identification à privilèges dont l'accès n'est accordé que si vous disposez d'une autorisation valide. Sans cette autorisation, même un administrateur PAM n'a pas le droit de voir les mots de passe et les clés SSH.

Outre le stockage, Axidian PAM vérifie régulièrement les mots de passe et les clés SSH pour s'assurer que les informations d'identification à jour sont stockées dans le système. Si une non-correspondance est détectée, l'administrateur recevra une notification appropriée.

Rotation des mots de passe et des clés SSH

Pour assurer la sécurité des mots de passe et des clés SSH, Axidian PAM les remplace par des clés aléatoires selon l'emploi du temps spécifié. Pour respecter les règles de sécurité de l'entreprise, vous pouvez configurer les paramètres de complexité du mot de passe généré.

Toutes les valeurs précédentes des mots de passe et des clés SSH sont également stockées à PAM dans l'histoire des mots de passe. Cela permet de «reculer» le mot de passe ou la clé à n'importe quel moment requis dans le passé. Cette fonction est nécessaire lorsque la ressource ciblée est restaurée à partir d'une copie sauvegardée et que vous devez utiliser les informations d'identification à jour au moment de la création de la copie sauvegardée.

Utilisation sécurisée des identifiants à privilèges

En introduisant Axidian PAM, les entreprises peuvent refuser explicitement l'utilisation des informations d'identification à privilèges par les employés. Les administrateurs de serveurs, de l'équipement réseau, Active Directory et des systèmes appliqués n'ont plus besoin de posséder des informations d'identification administratives, PAM résout cette tâche pour eux. L'employé se connecte à PAM à l'aide de son compte d'utilisateur, et sur la ressource ciblée, il ouvre une session sous le compte qui possède les droits nécessaires. Cette approche permet d'éviter l'utilisation incontrôlée de comptes à privilèges lorsque les employés peuvent les stocker dans un endroit dangereux (dans des fichiers sur le bureau ou le disque de réseau, sur des autocollants, etc.) ou transmettre spécialement des mots de passe aux tiers.

Pour les comptes à privilèges les plus importants, Axidian PAM vous permet d'activer le mode d'utilisation exclusive. Dans ce mode, une seule session peut être ouverte au nom d'un compte à privileges. Cela permet d'éviter les problèmes liés à la modification simultanée des systèmes administrés.

Technologie de l'entrée unique (Single Sign-On)

Axidian PAM vous permet d'ouvrir des sessions avec un transfert transparent des comptes administratifs à la ressource ciblée non seulement pour les protocoles d'accès à distance classiques tels que RDP, SSH ou Telnet. Le système comprend un agent SSO spécialisé (Single Signal-On Agent) qui permet de mettre automatiquement les comptes administratifs dans les formes de web- et des applications de bureau. En utilisant un agent, Axidian PAM peut fournir un accès transparent aux interfaces de web d'administration du matériel réseau, aux clients « épais » de la base de données et à d'autres applications.

Application pour l'application de la gestion des mots de passe

Les comptes administratifs dotés de pouvoirs étendus ne sont pas utilisés uniquement par les employés. De nombreux outils d'automatisation (applications, scripts, etc.) utilisent des enregistrements de service pour mettre en œuvre leurs fonctions. Pour éviter de stocker les mots de passe dans les scripts et les fichiers de configuration, Axidian PAM propose une interface logicielle (API) pour obtenir des comptes administratifs de service actuels. Toutes les opérations de réception des mots de passe seront enregistrées dans le journal PAM et les mots de passe seront modifiés pour une nouvelle valeur aléatoire à un intervalle de temps donné.

Réduction du nombre de comptes à privilèges

Le mécanisme Account Discovery détecte rapidement les comptes que les administrateurs et les employés de la sécurité numérique ont pu oublier (par exemple, les comptes administratifs temporaires qui n'ont pas été supprimés ou bloqués à temps). Un tel «inventaire » régulier permet de maintenir l'ensemble de comptes à privilèges en état actuel sans le rendre redondant. En retour, cela réduit la zone d'attaque potentielle des intrus et améliore la sécurité de l'information de la société.

En utilisant PAM, les sociétés peuvent refuser de créer des comptes administratifs personnels pour les administrateurs, réduisant encore le nombre des comptes administratifs à privilèges. Axidian PAM enregistre tous les événements d'accès aux ressources contrôlées où sont indiqués:

- membre du personnel ayant obtenu l'accès
- ressource à laquelle l'accès a été effectué

- compte administrative au nom duquel l'accès a été effectué
- date et heure d'accès
- durée de la session
- protocole d'accès utilisé.

Ainsi, même si vous utilisez des comptes impersonnels pour accéder aux ressources (administrateur, root, etc.), il restera dans PAM des informations sur les employés qui ont fait le travail.

Authentification multifactorielle

Lorsque les employés obtiennent un accès à privilèges, il est important d'appliquer des méthodes d'authentification fiables pour s'assurer que seuls les utilisateurs légitimes ont l'accès. Axidian PAM "de la boîte" prend en charge l'authentification à deux facteurs des utilisateurs en mode mot de passe + OTP (One-Time Password). Un mot de passe unique est généré par l'utilisateur dans l'application sur le smartphone.

Les entreprises qui utilisent les capacités de Windows pour authentifier les utilisateurs à l'aide de cartes à puce et de certificats numériques peuvent également utiliser cette approche pour l'authentification dans Axidian PAM.

Enquête des incidents

Pendant la realisation d'un accès à privilèges, il y a toujours le risque de perturber les systèmes d'information ou d'obtenir des comportements indésirables. En outre, pendant la réalisation des travaux par les maîtres d'œuvre il n y a pas toujours de sûreté que les travaux ont été exécutés correctement et dans leur intégralité. Dans telles situations, il est important de savoir quels changements ont été apportés au fonctionnement des systèmes et qui a produit les travaux.

Axidian PAM permet de capturer les actions des utilisateurs dans les formats suivants:

- Enregistrement vidéo - Enregistrement de l'écran complet du moniteur. Le système vous permet de personnaliser les paramètres d'enregistrement vidéo tels que la qualité d'image, sa netteté et la fréquence d'image.
- Captures d'écran - Captures d'écran périodiques. Cette fonction peut être utile pour économiser de l'espace de disque et enregistrer des sessions non critiques.
- Enregistrement de texte est le journal de texte de la session. Pour les sessions SSH, toutes les entrées/sorties d'utilisateur sont enregistrées, pour les sessions RDP les processus en cours d'exécution, les en-têtes des fenêtres actives et les entrées d'utilisateur sont fixés.

Les administrateurs PAM ont la possibilité de consulter les sessions en temps réel et après leur achèvement. Lors de l'affichage de la session active, l'administrateur peut la rompre s'il détecte un comportement suspect.

Les documents de la session (vidéos, captures d'écran, journal de texte) peuvent être téléchargés pour être consultés et analysés dans des outils tiers.

Axidian Privilege

Composition de Axidian Privilege

Figure 2. Structure de Axidian Privilege

Axidian PAM se compose des modules logiques et fonctionnels suivants.

Stratégies et autorisations

Les stratégies et autorisations définissent les paramètres d'accès à privilèges:

- à qui l'accès est accordé
- à quels comptes l'accès a été accordé
- à quelles ressources (serveurs et matériel) l'accès a été accordé
- pour quelle durée (de façon permanente/temporaire, pendant les heures de travail ou à tout moment)
- l'enregistrement des sessions à réaliser (enregistrement vidéo et texte, texte uniquement, captures d'écran, etc.)
- quelles ressources locales (disques, cartes à puce) seront mises à la disposition de l'utilisateur lors d'une session à distance
- si l'utilisateur est autorisé à voir le mot de passe du compte à privilèges

Les stratégies centralisées réduisent les coûts de l'administration du système et rendent les paramètres et les droits d'accès transparents pour les professionnels de la sécurité de l'information et les auditeurs. Pour plus de détails sur les stratégies et les autorisations, consultez la section “Contrôle d'accès centralisé.”

Comptes administratifs

Les comptes administratifs nécessaires à l'accès (logins, mots de passe, clés SSH) sont stockés dans un lieu où seul le serveur Axidian PAM a l'accès. Le stockage et la transmission des données à/de serveur sont effectués sous forme cryptée à l'aide d'algorithmes de cryptage résistants. L'accès au stockage est limité et n'est possible que pour le serveur PAM, et cette approche utilise une procédure spéciale pour « sceller » le serveur - hardening du serveur de base de données.

Les utilisateurs

Les utilisateurs PAM sont des employés qui bénéficient d'un accès à privilèges via le système PAM. Axidian PAM utilise Active Directory comme répertoire d'utilisateurs. Les comptes d'utilisateur sont utilisés pour accéder à la console utilisateur, au serveur d'accès, à SSH Proxy et à la console de gestion.

Les ressources

Une ressource dans Axidian PAM est un objet auquel l'accès est accordé. Dans la plupart des cas, ce sont des serveurs windows et linux. En outre, la ressource peut être une application distincte, par exemple pour la gestion de la base de données ou le configurateur Web du routeur.

Les sessions

Toutes les sessions d'accès à privilèges sont enregistrées et sauvegardées dans l'archive Axidian PAM. Dans l'archive des sessions, les enregistrements sont stockés sous forme cryptée et on ne peut y accéder qu'avec les pouvoirs appropriés au sein du système PAM. Les enregistrements sont conservés dans les formats suivants :

- L'enregistrement de texte est toujours en cours et enregistre les données suivantes:
  - l'entrée et la sortie complètes de la console dans les connexions SSH ;
  - tous les processus en cours d'exécution, les fenêtres ouvertes et les entrées de clavier pour les connexions RDP.
- L'enregistrement vidéo est effectué pour les connexions RDP et SSH. L'enregistrement vidéo n'est pas obligatoire, il est activé par l'administrateur PAM à l'aide du mécanisme de stratégie. La qualité vidéo est réglable et peut être différente pour les comptes différents. Par exemple, les sessions d'administrateur de domaine peuvent être enregistrées avec une qualité maximale et les sessions d'opérateur avec une compression.

- Les captures d'écran sont également effectuées pour les connexions RDP et SSH. L'enregistrement des captures d'écran n'est pas nécessaire, il est activé par l'administrateur PAM à l'aide du mécanisme de stratégie. La fréquence et la qualité des captures d'écran sont définies dans les stratégies.

La vue des sessions actives est disponible en temps réel avec la possibilité pour l'administrateur PAM de rompre la session.

Les rôles

Les rôles définissent les autorisations lorsque vous travaillez dans la console de gestion Axidian PAM. Le système a trois rôles par défaut:

- Administrateur - A un accès complet à toutes les fonctionnalités et paramètres de PAM.

- Opérateur - a le pouvoir de délivrer et de retirer les autorisations.

- Inspecteur - a l’accès à la lecture.

L'ensemble de privilèges pour chaque rôle peut être modifié et adapté aux besoins de l'organisation. En outre, vous pouvez créer vos propres rôles pour une délimitation plus fine des pouvoirs.

Journal des événements

Le journal des événements est stocké sur un serveur Axidian PAM spécial. Ces événements incluent toutes les activités des administrateurs et des utilisateurs PAM. Le journal enregistre qui a modifié et quels paramètres du système et sous quels comptes administratifs la connexion aux ressources ciblées a été effectuée.

Pour faciliter l'intégration dans SEIM et répondre à temps aux incidents, les événements peuvent être transmis via le protocole syslog à un serveur de magazine tiers.

Serveur d'accès

Le serveur d'accès met en oeuvre un modèle centralisé d'acquisition d'accès à privilèges. Tout d'abord, l'employé se connecte au serveur d'accès sur lequel ses droits sont vérifiés et une authentification à deux facteurs est effectuée, puis une session est ouverte sur la ressource ciblée.

Le serveur d'accès est alimenté par le serveur de bureau à distance Microsoft RDS (Remote Desktop Services) sur lequel les composants Axidian PAM sont installés. Lorsque l'utilisateur se connecte au serveur d'accès, une application spécialisée Axidian PAM est lancée en tant que l’emballage de bureau, qui réalise les fonctions suivantes :

- vérifie les droits d'accès de l'utilisateur - s'il est autorisé à accéder, sous le compte demandé, à la ressource cible demandée;
- authentifie l'utilisateur - l'utilisateur est tenu de fournir le deuxième facteur d'authentification avant l'ouverture de la session;
- fait un enregistrement vidéo de la session et des captures d'écran.

Le logiciel client suivant est utilisé pour ouvrir les sessions aux systèmes et applications ciblées sur le serveur d'accès :

- le client RDP Microsoft (mstsc) pour accéder au serveur Windows ;
- Navigateur pour accéder aux applications Web;
- Client PuTTY pour l'accès via les protocoles SSH et Telnet;
- Logiciel client spécialisé pour accéder aux systèmes d'information différents en utilisant des protocoles propriétaires (client « épais »).

SSH Proxy

SSH Proxy est une autre option pour obtenir l'accès via Axidian PAM sur le système Linux/Unix. Cette méthode présente les avantages suivants:

- n'est pas nécessaire d'utiliser Microsoft RDS ;
- possible d'utiliser n'importe quel client SSH ;
- client SSH travaille localement sur le poste de travail de l'employé.

SSH Proxy remplit des fonctions similaires à celles du serveur d'accès:

- vérifie les droits d'accès de l'utilisateur;
- authentifie l'utilisateur;
- fait un enregistrement de texte de la session (l'entrée/sortie ssh complète est enregistrée).

Si est utilize SSH Proxy, l'utilisateur initie la connexion à partir de son lieu de travail à l'aide d'un client SSH habituel. En tant que serveur de connexion, l'employé spécifie l'adresse SSH Proxy. Lors de la connexion au proxy de l'utilisateur, le deuxième facteur d'authentification est également demandé, puis une session est ouverte sur la ressource ciblée.

Filtre de commande

Pour les sessions SSH, l'administrateur PAM a la possibilité de définir les commandes autorisées ou interdites à exécuter sur certaines ressources ciblées (la liste de ressources est définie par la portée de la stratégie). Le filtre de commande peut être configuré pour fonctionner dans l'un des deux modes suivants:

- Tout ce qui n'est pas interdit est autorisé. Dans ce cas, l'administrateur identifie les commandes qui doivent être interdites de démarrer.
- Tout ce qui n'est pas autorisé est interdit. Un filtre plus strict dans lequel l'administrateur indique explicitement les commandes qui sont autorisées à démarrer, toutes les autres commandes sont bloquées.

Le mécanisme d'expression régulière est utilisé pour décrire les commandes. Les types de réactions suivants peuvent être spécifiés pour l'entrée d'une commande interdite:

- interrompre la session
- interrompre l'exécution de la commande.

SFTP и SCP[1]

En plus d'être accessible via le protocole SSH, SSH Proxy vous permet de vous connecter aux ressources ciblées via les protocoles SFTP et SCP. Dans ce cas, la connexion est effectuée de la même manière que SSH : en tant que serveur de connexion, l'employé indique l'adresse SSH Proxy. Lors de la connexion au proxy de l'utilisateur, le deuxième facteur d'authentification est également demandé, puis une session est ouverte sur la ressource ciblée.

Lorsque vous utilisez les protocoles SFTP et SCP, SSH Proxy crée un journal de session qui enregistre les opérations de fichiers effectuées par l'utilisateur.

Serveur de gestion PAM

Le serveur de gestion PAM est le module central du système Axidian PAM et assure l'échange de données et le fonctionnement des autres modules. Les principales tâches que le serveur résout sont les suivantes:

- Gestion centralisée de toutes les données du système (utilisateurs, ressources, comptes administratifs, autorisations, stratégies, etc.).

[1] The SFTP and SCP support will be added in v.2.7 in III quarter 2022.

- Cryptage des données critiques dans la base de données PAM (comptes administratifs à privilèges, etc.).

- Réalisation des tâches planifiées (recherche de comptes, rotation de mots de passe, etc.).

- API pour l'intégration avec des systèmes tiers.

Identity Provider (IDP)

Le module IDP (Identity Provider) permet de réaliser l'authentification des utilisateurs à deux facteurs lorsqu'ils accèdent à tous les composants du système. Le premier facteur d'authentification est le mot de passe de domaine de l'utilisateur, le second - le mot de passe à usage unique (OTP) généré dans l'application sur le smartphone.

Lorsque vous vous connectez pour la première fois à la console de gestion ou à la console d'utilisateur, l'employé est invité à enregistrer une application de génération de OTP. Une fois l'inscription réussie, l'employé a l'accès au système.

En plus des utilisateurs, IDP est responsable de l'authentification des applications qui utilisent API du serveur PAM.

Les connecteurs

Les connecteurs assurent un certain nombre de fonctions de gestion des comptes à privilèges:

- Recherche périodique de nouveaux comptes à privilèges sur les ressources ciblées. Cette mesure vous permet de vous protéger contre un administrateur malhonnête qui s'est créé un compte pour contourner le système PAM.

- Vérification périodique des mots de passe et des clés SSH des comptes à privilèges . Cette fonction vous permet de vous assurer que le stockage PAM contient des comptes administratifs actuels et que l'administrateur malhonnête n'a pas réinitialisé le mot de passe du compte administrative pour l'utiliser en contournant PAM.

- Modification périodique des mots de passe et des clés SSH. Indeed PAM génère des mots de passe complexes aléatoires et des clés SSH pour des comptes administratifs à privilèges contrôlés, les protégeant des accès non autorisés.

- Réinitialisation du mot de passe du compte administratif après l'avoir affiché à l'utilisateur. L'administrateur PAM peut autoriser aux employés à consulter le mot de passe du compte à privilèges lorsqu'une utilisation explicite du mot de passe est nécessaire. Une fois que l'employé a reçu le mot de passe, après un laps de temps donné, Axidian PAM réinitialise le mot de passe dans une nouvelle valeur aléatoire.

Axidian PAM comprend des connecteurs pour les systèmes ciblés suivants:

- connecteur au Directoire Actif (Active Directory);

- connecteur à Windows et Serveur de Windows;

- connecteur SSH pour se connecter aux systèmes Linux/Unix basés sur les distributions différentes;

- connecteur à la base de données (MS SQL, Oracle, PostgreSQL, etc.).

Console de gestion

La console de gestion fournit une interface de configuration et d'audit du système et se présente sous la forme d'une application Web. À l'aide de la console, l'administrateur permet aux utilisateurs d'accéder aux comptes administratifs et aux ressources, de configurer les stratégies d'accès et de consulter les journaux d'événements et lesenregistrements des sessions à privilèges. La console permet également aux administrateurs PAM de visualiser les sessions actives en temps réel et de mettre fin à la session de l'employé si nécessaire. L'accès à la console de gestion se fait par l'authentification à deux facteurs.

Console d'utilisateur

La console d'utilisateur se présente sous la forme d'une application Web. Toutes les autorisations délivrées à l'employé sont disponibles dans la console et vous pouvez rechercher l'adresse ou le nom de la ressource, le protocole de connexion ou le nom du compte. Après avoir trouvé la ressource nécessaire pour se connecter, l'utilisateur télécharge le fichier RDP avec les paramètres nécessaires. Ce fichier peut être sauvegardé et réutilisé, il n'est pas nécessaire de télécharger un nouveau fichier chaque fois. Pour les ressources SSH, vous pouvez copier la chaîne de connexion dans le presse-papiers pour l'utiliser dans un client SSH aléatoire.

Dans la console, l'utilisateur peut également voir les comptes administratifs à privilèges pour lesquels il a obtenu des autorisations. L'accès à la console se fait par l'authentification à deux facteurs.

Caractéristiques principales de l'Axidian Privilege

Protocoles d'accès RDP	RDP SSH HTTP(s) Telnet SFTP SCP Tout protocole via la publication du client
Types d'informations des comptes	Login + mot de passe pris en charge Clé SSH
Recherche de comptes à privilèges et gestion du mot de passe	Windows Linux Active Directory DBMS (MS SQL, PostgreSQL, MySQL, Oracle, etc.)
Répertoires d'utilisateurs pris en charge	Active Directory
Technologies d'authentification à deux facteurs	Mot de passe + TOTP (générateur de logiciels)
Types d'enregistrement de session pris en charge	Journal de texte L'enregistrement vidéo Captures d'écran
Technologie d'accès à distance	Microsoft RDS SSH Proxy

Sur la société Axidian

Axidian (axidian.com) est un développeur de logiciels ayant 10 ans d'expérience dans le domaine de la sécurité de l'information. Nos experts ont réalisé des dizaines de projets pour des entreprises des secteurs différents: banques et institutions financières, télécommunications, énergie, transports, institutions officielles et éducatives. Nos bureaux principaux sont situés en UAE, Lituanie et au Singapour.

Distributeur à valeur ajoutée de solutions IT

Cybersécurité | Réseaux | Wi-Fi | Stockage

HAFS NETWOKS,
Représente et accompagne les éditeurs et les constructeurs pour créer de la proximité auprès des partenaires et des clients finaux.

Notre objectif :
Proposer des solutions qui repondent aux besoins. Accompagner, former et développer pour accroître le rayonnement sur le marché français et en Afrique sub-sahérienne.

Solutions **Formations** **Services**

Portfolio Solutions

Portfolio Solutions

HAFS
Distributeur à valeur ajoutée

Site web : www.hafs-networks.com

France
sales@hafs-networks.com
+33 (0)6 51 10 87 49 / (0)9 74 98 52 96

Côte d'Ivoire
sales-ci@hafs-networks.com
+225 07 89 82 56 49 / +225 07 59 05 85 82