cyberelements

PAM : Les 4 épines des accès prestataires

1

Pourquoi le PAM s'impose comme indispensable pour mes infogéreurs ?

On assiste depuis plusieurs années maintenant à une démultiplication des accès prestataires vers un nombre lui aussi croissant de ressources informatiques accédées au sein des entreprises infogérées. Ces accès distants ne sont pas sans risques pour les entreprises : une étude Opus & Ponemon Institute a révélée que **59% des organisations ont subi une fuite de données causée par l'un de leurs prestataires.**

Afin de contrer ces risques de plus en plus prégnants pour les entreprises, le déploiement de solutions adaptées aux enjeux des accès prestataires devient alors un **impératif pour la sécurité globale des systèmes d'informations**. Il s'agit pour les entreprises d'être capable de maitriser tous les accès et non plus seulement ceux émanant de ses collaborateurs.

Maîtriser et surveiller les accès prestataires grâce au PAM (Privileged Access Management)

Surveillance des accès et des actions d'administration

Les solutions de PAM permettent de **contrôler et surveiller les accès et les actions des utilisateurs à pouvoirs** (dont font partie les prestataires informatiques), c'est-à-dire des utilisateurs ayant des droits particuliers leur permettant d'accéder à des ressources critiques du système d'information et de mener des actions sur ces ressources critiques.

Concrètement, les solutions de PAM permettent de surveiller les actions de tous les prestataires informatiques lorsqu'ils se connectent (nominativement) sur le réseau administré. Ces accès nominatifs bénéficient alors de l'**approche Zero Trust** qui permet de ne donner que le strict nécessaire en termes de droits d'accès et ouverture réseau afin de limiter fortement les risques induits par ces accès. Toute solution qui évite l'ouverture de ports réseaux et qui se situe à un niveau applicatif (couche 7 du modèle OSI) doit ainsi être privilégiée.

Enregistrement des sessions

Les actions des prestataires informatiques sont ensuite **enregistrées sous format vidéo**, ce qui permet à la DSI de l'entreprise infogérée de **voir en temps réel** ou de **revoir** le déroulement d'une intervention **a posteriori**. Pour simplifier la recherche d'une action spécifique parmi l'ensemble des vidéos enregistrées, la **recherche avancée** permet quant à elle de définir le type d'action à retrouver et ainsi afficher toutes les vidéos ainsi que le moment précis où cette action est effectuée. L'intérêt est de pouvoir retrouver très rapidement la source d'une compromission, d'une erreur ou encore d'une preuve d'action sur le système d'information infogéré.

Par ailleurs, et pour aiguiller le responsable informatique dans son contrôle a posteriori des sessions, un **score de vigilance** est appliqué à chaque vidéo afin qu'il puisse repérer en un coup d'œil les sessions contenant des actions sensibles qu'il pourra contrôler et visionner en priorité.

2

Pourquoi le PAM est un rempart efficace contre les menaces ?

Les prestataires informatiques doivent accéder aux ressources critiques des entreprises infogérées. Cet accès large aux ressources constitue une menace de **propagation de malwares** s'ils se font via des solutions inadaptées à la criticité des actions réalisées.

Et lorsque la bonne solution est déployée, certaines fonctionnalités ou spécificités produit permettent de **diminuer encore davantage les risques cyber pour le système d'information infogéré.**

Recourir à une solution nativement destinée aux accès distants

Sécurisation native des flux de connexions

Les accès prestataires étant par essence des accès distants, la solution de PAM retenue doit être capable de **nativement sécuriser les flux de connexions**, par exemple via un flux de type **ZTNA** (Zero Trust Network Access) qui ne donne accès qu'exclusivement à la ressource administrée et non à l'ensemble du SI et qu'au moment où on accède à ladite ressource, ce qui limite la surface d'attaque depuis l'extérieur de la structure.

De plus, il est primordial de **rendre les ressources invisibles du réseau Internet tout en permettant d'y accéder** : la technologie de réécriture d'URL le permet. Cette architecture permet la **rupture protocolaire** grâce à un mécanisme à double barrière avec un composant dans le cloud et un composant dans le LAN de l'organisation : il n'y a qu'un flux sortant qui est créé sans ouverture de port réseau. Deux tunnels sécurisés sont ouverts pour le fonctionnement de ce module : un tunnel entre le terminal utilisateur et le service cloud et un tunnel entre le service cloud et le relais localisé dans le LAN de l'organisation. Le seul composant exposé à l'extérieur est le composant situé dans le cloud qui ne permet pas à lui seul d'accéder aux ressources administrées.*

Accès sans agent

Ces accès externes ne doivent également pas nécessiter le déploiement d'un agent sur le poste, non seulement dans une logique de **simplification** des accès sécurisés des prestataires, mais aussi pour répondre à un besoin de **scalabilité** étant donné la multiplication d'accès distants auxquels les entreprises doivent régulièrement faire face.

3

Pourquoi mettre en place une solution de PAM dans le cloud ?

Une fois la solution identifiée, l'enjeu est de la **déployer rapidement** pour protéger un système d'information encore à la merci de potentielles fuites de données ou encore propagations de malwares résultant des accès prestataires.

Le recours à une solution de PAM en service cloud public (**PAM as a Service**) répond à cet impératif en permettant un **déploiement de la solution en quelques clics** avec un impact minime en termes d'allocation de ressources humaines aussi bien lors du déploiement que pour l'administration de la solution grâce à des mises à jour régulières et automatiques totalement transparentes pour la DSI.

Tirer parti de la flexibilité du cloud

Simplification et rapidité de déploiement

Le PAM as a Service représente, pour la plupart des entreprises ne disposant pas encore de solution de PAM, la meilleure approche pour s'attaquer à la surveillance des accès prestataires. Le premier avantage du PAM as a Service est sa **simplicité et rapidité de déploiement** ainsi que les **gains de temps** qu'il procure **sur le long terme**. La majorité du service est hébergé sous forme de service cloud, notamment pour le portail d'accès des utilisateurs, afin de garantir un accès en toute sécurité y compris en situation d'accès externe.

Ensuite, un relais est déployé au plus proche des ressources pour sécuriser la connexion de bout en bout. Le relais se référence ensuite automatiquement sur le serveur centralisé. Une fois le ou les relais mis en place, aucune installation supplémentaire n'est nécessaire. Les **mises à jour** sont ensuite **automatiques** et **totalement transparentes pour la DSI**, ce qui permet de ne pas mobiliser des ressources humaines pour des tâches liées à la gestion de la solution.

Gain financier

Le PAM as a Service a aussi un intérêt financier : **les dépenses sont échelonnées dans le temps** en fonction de l'usage réel là où le PAM on-premise nécessite un investissement de départ important parfois incompatible avec les budgets IT alloués. La maintenance et la gestion des mises à jour de la solution vont également être un vecteur de coût dans le modèle on-premise. Le PAM as a Service permet en définitive d'avoir une **meilleure prédictibilité des coûts** et de **les étaler dans le temps.**

Afin d'optimiser cet intérêt financier, il peut être également judicieux de souscrire à une solution de PAM proposant un **licensing à utilisateurs simultanés**. Par exemple, si une entreprise à 10 utilisateurs à privilèges (internes ou externes) mais qu'en pratique pas plus de 5 d'entre eux sont connectés en même temps, seules 5 licences seront nécessaire ce qui limite alors le coût de la souscription.

4

Pourquoi le PAM Cleanroom simplifie votre gestion IT ?

Pour les entreprises il est parfois tentant de multiplier les outils de cybersécurité pour s'assurer d'être en mesure de parer à toutes les menaces. **Cette multiplication de solutions de cybersécurité est pourtant contre-productive :** une étude d'IBM Security a effet révélé que pour les organisations avec plus de 50 outils de cybersécurité l'opportunité de détecter des cyberattaques baisse de 8% et celle d'y répondre de 7% par rapport aux entreprises disposant de moins de 50 solutions de cybersécurité. Une autre étude, réalisée par Trend Micro, corrobore ces observations puisqu'elle révèle que pour les collaborateurs travaillant dans les centres opérationnels de cybersécurité, l'excès de solutions entraîne plutôt une série d'effets négatifs, notamment une baisse de confiance dans la capacité à prioriser et répondre aux nombreuses alertes ou encore une augmentation du temps passé à traiter des faux positifs.

Pour optimiser la sécurité des accès prestataires, et dès lors que le ou les outils choisis sont adaptés à ces accès spécifiques, **le recours a un nombre réduit de solutions est donc primordial** pour garantir une cyber résilience de l'organisation infogérée.

Fournir aux prestataires une expérience unifiée et sécurisée de bout en bout

Consolidation d'un ensemble de fonctionnalités

La sécurisation des accès prestataires doit donc, pour gagner en efficacité opérationnelle, passer par le déploiement d'une **solution unique**, capable de consolider un ensemble de fonctionnalités dédiées à la sécurité des accès externes et à la surveillance des utilisateurs à pouvoirs. La solution choisie doit donc être en mesure d'authentifier nominativement les prestataires via **MFA** et proposer un **coffre-fort de mots de passe** pour protéger l'organisation des fuites de mots de passe émanant de ces prestataires et empêcher les connexions non identifiées.

Les accès distants de ces prestataires doivent être sécurisés, notamment en y appliquant le **principe de moindre privilège** consistant à limiter leurs droits et habilitations sur le système d'information aux seules applications et données qui leurs sont nécessaires dans le cadre et pour la durée de leurs missions. L'intégration native d'accès distants sécurisés comme le **ZTNA** au sein de la solution de PAM est même incontournable lorsqu'il est question d'accès distants de prestataires informatiques.

La solution doit être capable de **tracer et d'enregistrer l'ensemble des actions des prestataires** et permettre à la DSI d'interrompre toute action en temps réel (automatiquement ou via intervention humaine) si besoin. Il s'agit là d'avoir un contrôle total de toutes les actions d'administration, seul moyen de véritablement maîtriser la sécurité du système d'information de l'entreprise.

Ergonomie et maitrise de l'ensemble du cycle de vie des prestataires

Et puisque la sécurité va souvent de pair avec la simplicité d'utilisation, le recours à un **portail d'accès HTML5** ne nécessitant pas le déploiement d'agent sur le poste du prestataire, de même que la mise à disposition d'une plateforme d'administration intuitive pour la DSI, sont tout aussi importants que les fonctionnalités inhérentes à la solution de PAM.

Enfin, pour s'assurer que des anciens prestataires n'opérant plus sur le SI n'aient plus aucun accès à celui-ci, la solution de PAM doit proposer une fonctionnalité de **découverte des comptes** qui permet, en scannant le réseau d'administration à intervalles réguliers, de détecter tous les comptes d'administration dont les comptes **shadow admin** et de soit les réintégrer dans la liste des comptes officiels (et y apporter les mécanismes de contrôle et de traçabilité) soit les supprimer.

Surveiller et sécuriser les actions d'administration sur le SI

cyberelements

La plateforme Zero-Trust fournit à tous les types d'utilisateurs (employés au bureau, travaillant à distance, tiers, opérateurs OT) un accès transparent et immédiat (standard, privilégié, local, distant) à toutes les ressources dont ils ont besoin pour travailler (applications cloud, postes de travail, applications distantes, données, infrastructures IT&OT, services).

Essayer gratuitement