FAMILLES DE PRODUITS

Gestion des accès à privilèges (PAM)

Le volet cyber de France Relance

L'Agence nationale de la sécurité des systèmes d'information (ANSSI) est en charge du volet cybersécurité de France Relance pour concevoir des offres de service destinées à **élever le niveau de cybersécurité de l'État, des collectivités territoriales et des organismes au service des citoyens** (social, santé, formation, audiovisuel, sécurité).

Les appels à projets, l'une des réponses de l'ANSSI au volet cyber de France Relance

Différentes solutions ont déjà été identifiées par l'ANSSI comme pouvant faire l'objet d'un projet d'acquisition dans le cadre du plan France Relance :

Analyse de risque EBIOS Risk Manager	Bug Bounty	Endpoint Detection and Response	Gestionnaire de vulnérabilités	**Gestion des accès à privilèges (PAM)**
Pare-feu applicatif web (WAF)	Sauvegarde sécurisée	Sécurisation de l'Active Directory	Sécurisation de la messagerie email	Gestionnaire de mots de passe

La solution de gestion des accès à privilèges

74%
des fuites de données impliquent l'utilisation illicite d'un compte à privilège (*)

Qu'est-ce qu'une solution de gestion des accès à privilèges ?

Les solutions de **gestion des accès à privilèges (PAM)** sont des solutions visant **à gérer et protéger les comptes utilisateurs possédant de forts privilèges** (administrateurs internes et prestataires) et à **gérer les accès d'administration aux équipements** d'un SI.

Une solution de PAM peut englober plusieurs composants, les plus courants sont :
- un **bastion**, composant principal qui servira d'intermédiaire entre un administrateur et une ressource,
- un **coffre-fort de mots de passe** pour stocker les informations d'accès aux ressources,
- un **portail d'accès web**, pour simplifier et sécuriser les accès externes.

Le déploiement d'un PAM permet **de contrôler et de surveiller les actions effectuées** par les utilisateurs privilégiés sur un actif donné. Les principales fonctionnalités que l'on retrouve dans un PAM sont **la gestion centralisée des accès privilégiés**, la rupture protocolaire (l'accès indirect aux équipements), la mise à disposition d'**un coffre-fort de mots de passe** lié aux accès et un **système d'enregistrement des sessions ou des logs** pour toujours garder une trace des activités effectuées par les utilisateurs à hauts privilèges.

(*)privileged-access-management-the-key-to-protecting-your-business-amid-cybercrimes-current-boom (broadcom.com)

Pourquoi cette famille de solution ?

- **Les comptes à forts privilèges sont des cibles de choix** car la compromission de l'un d'entre eux multiplie les actions que les attaquants peuvent mener dans le SI.
- Un PAM permet de **centraliser la gestion des accès à hauts privilèges et empêcher les connexions directes aux équipements**.
- De telles solutions permettent de **connaitre et de maîtriser les comptes à privilèges** du SI.
- Chaque connexion ou action liée à un compte à privilège géré par un PAM **donne lieu à des traces** (enregistrement de session, logs).
- Grâce au **coffre-fort intégré** dans les PAM, les utilisateurs n'ont pas besoin de connaître les identifiants et mots de passe nécessaires pour se connecter aux systèmes à administrer.
- Les solutions présentes dans cette famille sont adaptées à des organisations possédant une **maturité sécurité avancée**.

Menaces couvertes

Menaces internes
(Absence de gestion des droits et utilisateurs, partage de mots de passe)

Menaces externes
(Usurpation d'identité, compromission d'un prestataire)

Périmètre

Comptes à privilèges

Maturité sécurité attendue pour la solution

Basique → Importante → **AVANCÉE** → Spécifique

Déploiement (1/2)

1. Lister les comptes utilisateurs, les ressources et les droits respectifs des utilisateurs sur ces ressources
   Concevoir une matrice des flux nécessaires entre les utilisateurs et le PAM, ainsi qu'entre le PAM et les ressources à protéger
2. **[Option] : Déployer plusieurs bastions pour assurer une haute disponibilité** (+)
   Déployer les composants du PAM sur un socle physique ou virtuel (+)
   [Option] : Déployer une interface de gestion unique en cas de mise en place de multiples bastions
3. Configurer des politiques de sécurité et des restrictions liées aux actions d'administration (plage horaires, commandes interdites…)
4. Superviser et gérer les actions d'administration à travers les logs et enregistrements (+)
   [Option] : Intégration avec un SIEM ou un SYSLOG

Déploiement (2/2)

Phase de BUILD

- **Équipe d'intégration** nécessaire pour l'installation d'une ou plusieurs appliances et l'intégration du PAM avec les solutions tierces
- **Équipe d'intégration** nécessaire pour la configuration des accès, des utilisateurs et de la journalisation
- **Administrateur réseau** pour ouvrir les flux nécessaires au bon fonctionnement de la solution et la mise en place d'une interconnexion VPN en cas d'ouverture aux prestataires

Complexité : moyenne

Phase de RUN

- **Administrateur de la console** nécessaire pour la gestion et visualisation des accès
- **Administrateur système** nécessaire pour le maintien en condition opérationnelle de l'outil
- **Support éditeur** pour assister les clients en cas de questions ou d'incidents

Complexité : moyenne

Recommandations d'usage (1/2)

- La solution PAM **ne doit pas être localisée sur un SI de faible niveau de confiance** et la conception du réseau doit obliger son usage systématique lorsqu'un administrateur souhaite atteindre les ressources à administrer.
- Le bastion **ne doit pas être exposé sur internet**, les accès externes doivent d'abord passer par un VPN ou un composant dédié pour accéder à la solution.
- **Des processus d'arrivées et départs** doivent être mis en place pour gérer efficacement les comptes utilisateurs renseignés dans le PAM.
- **Le principe du moindre privilège** doit être appliqué aux utilisateurs du PAM.
- **Une revue des comptes utilisateurs** doit être effectuée de manière régulière (minimum 1 fois tous les 6 mois).
- Le PAM est une ressource critique, **le principe de défense en profondeur** doit donc être appliqué autour de ce dernier, et une procédure bris de glace doit être implémentée.
- Les actions des utilisateurs doivent être **contrôlées et surveillées.**

Recommandations d'usage (2/2)

- Les postes qui accèdent aux PAM doivent être **durcis** et ne doivent **pas pouvoir accéder à Internet, ni à une messagerie.**
- La base des comptes contenue dans un bastion doit être homogène (ne pas mélanger les comptes Tier 0 avec les comptes Tier 1 ou Tier 2). Le modèle en tiers a pour but d'éviter le regroupement de comptes d'accès pour des ressources de criticité différente. Les différents tiers du modèle se définissent généralement de la manière suivante :
  - Tier 0 pour les accès liés aux contrôleurs de domaines
  - Tier 1 pour les accès privilégiés liés aux serveurs et applications
  - Tier 2 pour les accès privilégiés sur les environnements utilisateurs
- Il faut protéger les accès au portail/API d'administration du PAM et les dédier aux seuls postes/personnes autorisés.

Complémentarité avec d'autres outils

Comment optimiser l'efficacité de la solution ?

- SIEM (centralisation des alertes)

Quelles autres solutions celle-ci peut-elle compléter ?

- Firewall & cloisonnement réseau
- Un VPN pour permettre un accès externe jusqu'au PAM

Services associés

Pilotage de la solution possible par un tiers pour :

- Le déploiement et la configuration du PAM
- Exploitation de l'outil au quotidien (dans le cadre d'une infogérance)
  - Le PAM est une solution sensible qui centralise comptes, mots de passe et accès à hauts privilèges. Avant de déléguer sa gestion, le bénéficiaire doit mener une étude des risques et s'assurer que la prestation réponde aux enjeux de sécurité et qualité attendus.
- Intégration des logs de l'outil dans un SIEM / SOC géré par un tiers