Une sécurité parfaite pour l'accès à distance

Qu'est-ce que le Privileged Access Management (PAM), quel usage et quel fonctionnement? Bernhard Aregger, sales specialist chez le distributeur de sécurité informatique BOLL, explique la fonction et l'utilité des solutions PAM à l'exemple de la solution Fudo PAM.

Pourquoi a-t-on besoin d'une solution de Privileged Access Management (PAM)?
Lors du premier contact avec les personnes intéressées par une solution PAM, je pose toujours la question initiale suivante: savez-vous exactement qui accède à vos systèmes tels que les pare-feu, les serveurs ou les bases de données, ce qui se passe et quand l'accès a eu lieu? Compte tenu du nombre généralement élevé de comptes d'utilisateurs avec accès privilégié – par exemple pour les prestataires de services externes – la vue d'ensemble fait souvent défaut et les entreprises ne peuvent plus gérer manuellement la gestion des accès.

Et qu'apporte concrètement une solution PAM?
Les solutions PAM comme Fudo PAM rendent l'invisible visible, elles créent une visibilité complète sur les sessions à distance, aident à identifier et à bloquer les activités nuisibles et soutiennent ainsi les exigences de conformité respectives. Fudo PAM n'est pas seulement intéressant pour les grandes entreprises, mais aussi pour les PME, car le nombre de systèmes concernés ne cesse d'augmenter. Et ce sont justement les PME qui font de plus en plus appel à des spécialistes externes pour gérer et entretenir leurs systèmes à distance. Une raison de plus pour sécuriser au mieux tous les accès privilégiés.

Comment fonctionne la solution de Fudo?
Fudo PAM se connecte sous forme d'appliance matérielle ou de machine virtuelle entre les utilisateurs à distance et les systèmes de l'entreprise et enregistre de A à Z toutes les sessions des utilisateurs. Le monitoring continu des sessions avec enregistrement permet de tout suivre, même après coup, jusqu'à la moindre frappe de clavier. Parallèlement, l'IA intégrée analyse le comportement de l'utilisateur et peut ainsi détecter et empêcher toute activité suspecte. La solution offre d'autres fonctions telles que le secret manager pour la gestion automatisée des mots de passe et l'efficiency manager.

Quel est le rôle de l'efficiency manager?
Il analyse le niveau d'activité pendant une session. On peut ainsi savoir si un prestataire de services s'est connecté pendant des heures mais sans faire grand-chose. Il est de la sorte possible de lutter contre les surfacturations, comme c'est souvent le cas dans la pratique. L'efficiency manager est une fonction supplémentaire utile. Toutes les fonctions mentionnées sont comprises dans la licence et ne doivent pas être achetées séparément.

Bernhard Aregger, sales specialist chez le distributeur de sécurité informatique BOLL.

En quoi Fudo se distingue-t-il des autres solutions PAM?
Tout d'abord par sa méthode d'enregistrement. Contrairement aux solutions comparables, Fudo PAM ne crée pas d'enregistrement vidéo, mais conserve les données brutes, c'est-à-dire la communication dans les protocoles natifs comme RDP, VNC, SSH, Telnet, HTTP/HTTPS ainsi que les protocoles de base de données et OT comme Modbus SCADA. Les enregistrements occupent ainsi beaucoup moins d'espace mémoire. Une session de huit heures nécessite en général 20 ou 30 mégabytes contre plusieurs gigabytes pour un enregistrement vidéo.

Quels sont les autres avantages de l'enregistrement des données brutes?
La fonction OCR intégrée permet une recherche textuelle rapide sur l'ensemble des sessions. On trouve les activités recherchées en quelques secondes et on ne doit pas passer des heures à fouiller dans les enregistrements vidéo. On peut ainsi réagir beaucoup plus rapidement après une infraction. A l'aide «d'expressions régulières», il est possible de faire en sorte qu'une session soit automatiquement stoppée ou que l'administrateur reçoive un avertissement lorsque certains termes apparaissent. Enfin, les données brutes sont dotées d'un timecode et donc difficilement manipulables.

Quelles sont les autres caractéristiques de Fudo?
Fudo – qui n'est d'ailleurs pas une entreprise américaine, mais un fabricant européen dont le siège principal et le bureau de développement se trouvent à Varsovie – a voulu créer une solution simple et épurée. C'est ce que l'on constate en regardant le produit de plus près: il est clair et structuré, conforme au RGPD et se concentre entièrement sur la sécurisation des accès privilégiés, la gestion des droits d'accès et la surveillance des sessions. Associé à une architecture sans agent, cela se traduit par une implémentation rapide. Fudo PAM peut être mis en place en quelques heures, sans interruption des services informatiques. Le réglage précis s'effectue ensuite en cours de fonctionnement. En outre, la solution est compatible avec le cloud en tant qu'appliance virtuelle et peut être utilisée pour des services managés.

BOLL
IT Security Distribution

BOLL Engineering SA
En Budron H15 | 1052 Le Mont-sur-Lausanne
Tél. 021 533 01 60 | vente@boll.ch | www.boll.ch