

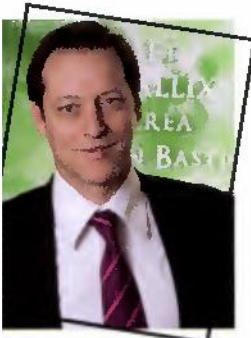


Wallix « trace » les flux de données tout en gérant les accès



À l'image d'une caméra vidéo, les outils de Wallix surveillent et enregistrent en temps réel tout mouvement qui entre et sort du réseau informatique de l'entreprise. Et chaque session peut être restituée sous forme d'image. L'un des intérêts du système est là : offrir une traçabilité incontestable en cas d'audit ou d'incident.

TEXTE : FÉLICIE D'ORGEVAL, PHOTOS : WALLIX.



Jean-Noël de Galzain,
PDG de Wallix.

Les sociétés capables d'offrir la surveillance du trafic informatique de l'entreprise en temps réel se comptent sur les doigts de la main à travers le monde. Parmi elles, Wallix – jeune entreprise qui vient d'obtenir le statut de gazelle – se distingue par des spécificités techniques qui donnent à ses logiciels un avantage certain.

« Notre principal outil, le Wallix AdminBastion, une fois installé derrière le pare-feu, est prêt à l'emploi. En effet, contrairement à ce qui existe actuellement sur le marché, le WAB ne nécessite aucun agent pour fonctionner, ni sur les postes de travail ni sur les équipements administrés, ce qui diminue d'autant son coût de déploiement », assure Jean-Noël de Galzain, PDG de Wallix, société membre du pôle Systematic.

Les principales fonctions du WAB permettent de savoir qui fait quoi, quand, où et comment

grâce au suivi des connexions en temps réel. Les actions effectuées sur les équipements cibles sont enregistrées en continu, avec possibilité de les visionner ultérieurement au format Flash Vidéo pour les sessions graphiques Windows Terminal Server (RDP), au format texte pour les sessions en lignes de commandes (SSH, Telnet).

L'analyse des flux SSH permet de percer un système d'authentification forte. Une alerte, voire une coupure automatique de la connexion SSH peut être programmée en cas de détection d'une chaîne de caractères interdite.

Une authentification unique

Le contrôle d'accès aux équipements de l'entreprise se fonde sur les règles qu'elle décide de mettre en œuvre. Ces règles se basent sur des critères tels que l'adresse IP, l'identifiant, les plages horaires, les protocoles ou le type de session SSH (X11, Shell, Remote exec...). En cas de connexion vers des équipements identifiés comme critiques, une alerte est donnée par le WAB quand l'authentification échoue ou quand la connexion automatique à un compte cible est impossible.

« Enfin, intérêt important du système, chaque utilisateur se connecte au WAB avec son identifiant et son mot de passe pour accéder ensuite aux équipements cibles autorisés sans avoir à s'authentifier une seconde fois. Les mots de passe de ces équipements sont stockés dans le WAB et permettent d'automatiser l'ouverture de sessions », souligne Jean-Noël de Galzain. □

WALLIX PRÉPARE UNE LEVÉE DE FONDS

La création de deux filiales au Royaume-Uni et aux États-Unis ne suffit pas à Wallix, qui cherche à se déployer dans d'autres pays. Pour accélérer son déploiement international, la nouvelle gazelle prépare une levée de fonds de 3 à 5 millions d'euros. Son objectif est de passer de 20 vendeurs à valeur ajoutée aujourd'hui à 200 d'ici à cinq ans.

1. En informatique, un agent est l'équivalent d'un robot logiciel. C'est un programme qui accomplit des tâches à la manière d'un automate et en fonction de ce que lui a demandé son auteur (source : Wikipédia).