

Communiqué de presse
Paris, le 07 juin 2022

TheGreenBow renforce la sécurisation des postes de travail nomades avec des fonctionnalités Zero Trust

Lors du Forum International de la Cybersécurité à Lille (7-9 juin), TheGreenBow propose des démonstrations de nouvelles fonctionnalités Zero Trust sur son stand D12.

La gamme de Clients VPN TheGreenBow est conçue pour protéger les connexions en toutes circonstances. Pour accroître davantage encore le niveau de sécurité des connexions distantes que TheGreenBow ajoute des fonctionnalités ZTNA (Zero Trust Network Access) pour ses clients VPN Windows.

Face au défi toujours plus grand de la sécurisation des connexions distantes au SI, les RSSI cherchent des solutions pour conserver la maîtrise des postes utilisateurs. Le travail hybride s'imposant au sein des entreprises et des organismes publics, les salariés alternent leur présence au bureau avec le télétravail. Cette nouvelle organisation apporte beaucoup de flexibilité mais favorise également les usages numériques à risques, à commencer par l'usage à la fois personnel et professionnel des équipements du salarié. Avec la forte croissance des menaces cyber et des réglementations à respecter (RGPD, LPM, Directive NIS 2 ...), Les RSSI reconnaissent qu'il devient de plus en plus difficile de sécuriser les télétravailleurs.

Les fonctionnalités Zero Trust développées par TheGreenBow ont pour objectif de leur simplifier la tâche. En particulier, le « mode filtrant » et la conformité de poste sont deux fonctionnalités disponibles dans les versions à venir à partir de la prochaine version majeure du Client VPN Windows (la version 7) qui sera mise sur le marché en juin.

Le mode filtrant pour réduire la surface d'attaque

Cette fonctionnalité, une fois paramétrée, permet de protéger le poste de travail en réduisant au strict minimum les flux entrants et sortants autorisés. De plus, l'autorisation des flux est contextualisée en fonction de la posture du poste de travail. Des jeux de règles différents peuvent être appliqués si le poste est par exemple, en situation de nomadisme, ou connecté au réseau de l'entreprise. Une fois activé, le mode filtrant empêche également les connexions entrantes malveillantes.

La conformité de poste avant l'ouverture d'un tunnel VPN

Autre moyen d'accroître la sécurité : les points de contrôle effectués avant l'ouverture d'un tunnel VPN donnant l'accès au SI de l'entreprise. Dans ses versions 7, le client VPN Windows procède à un double contrôle. D'une part il vérifie que l'antivirus est bien à jour sur le poste et d'autre part, il s'assure que le firewall est également bien activé. Si une anomalie est détectée, le tunnel VPN n'est pas monté et l'utilisateur n'est pas autorisé à accéder au SI de l'entreprise.

Des configurations VPN spécifiques selon les utilisateurs

TheGreenBow étoffe sa gamme Secure Connection Management, qui comprend déjà un serveur d'activation, dans le but d'offrir la maîtrise et le contrôle nécessaires pour garantir un niveau de sécurité élevé des connexions distantes.

Au FIC 2022, TheGreenBow présentera en avant-première, un démonstrateur du Secure Connection Center : une console d'administration permettant de créer et déployer facilement et rapidement des configurations VPN sur les postes de travail en s'appuyant sur la gestion d'identité de l'entreprise. Grâce à elle, les administrateurs distribuent la bonne configuration au bon utilisateur et renforcent leur capacité d'affecter des droits d'accès distincts selon le profil des utilisateurs.

« Les tunnels IPsec garantissent la confidentialité et l'intégrité des données échangées. Mais face à la multiplication des pratiques numériques à risque, nous devons offrir plus à nos clients. C'est pourquoi nous intégrons davantage de fonctionnalités orientées Zero Trust dans nos produits afin d'aider les RSSI à maintenir un haut niveau de sécurité » résume Mathieu Isaia, Directeur Général de TheGreenBow.

A propos de TheGreenBow

Créé en 1998, TheGreenBow est un éditeur français de logiciels de Cybersécurité qui fournit des solutions VPN de confiance et dont l'expertise repose sur la sécurisation des communications. Premier opérateur à avoir été certifié CC EAL3+, qualifié standard et agréé DR OTAN et UE en 2013, pour son logiciel Client VPN Windows, TheGreenBow, l'acteur de référence des Clients VPN, distribue ses logiciels dans plus de 70 pays. Depuis fin 2019, TheGreenBow détient le label « *Utilisé par les armées françaises* » pour le produit Client VPN Windows Certifié. Ce label atteste de la mise en œuvre du logiciel par les services du Ministère des Armées Françaises.