Kirébos

Application de contrôle réseau :
Limiteur de connexion Wifi et internet

Kirébos est un firewall (Pare-feu) permettant de bloquer les connexions wifi ou internet sur un réseau local, une infrastructure ou permet de limiter les accès indésirables à un ordinateur, une tablette, un téléphone portable.

Fonctionnement :
Le programme permet de fermer l'accès au réseau en clôturant l'accès par l'intégration du matériel présent dans l'infrastructure ou le réseau qu'il soit aérien ou filaire. L'application est intégrée au serveur afin de ne pas compromettre le réseau plus loin qu'à son point de connexion de base envoyant le signal. S'il s'agît d'un téléphone portable alors, le programme est intégré afin que le partage de connexion ou l'accès à une quelconque connexion demande une authentification basée sur les éléments de référence 4G, 3G, 2G, Wifi, Connexion Lte (limitée ou d'urgence) du constructeur ou du système d'exploitation.

Les données sont conservées durant 2 ans afin de pouvoir constater d'un quelconque changement sur la ligne. Le système permettant de déclarer à l'opérateur téléphonique ou au fournisseur internet toute défaillance de sécurité, besoin d'intervention sur la ligne ou le forfait ainsi que la présentation d'un rapport de piratage informatique au centre de cybermalveillance du ministère de l'intérieur.

Descriptif :
Cette application permet de restreindre le réseau aux matériels faisant partie de la structure à sécuriser et empêche l'accès tiers ou les connexions sauvages via le Wifi ainsi que par l'accès par internet via le serveur.

Le limiteur fonctionne sur la base de la reconnaissance des adresses Mac et les adresses IP du matériel connecté. Le réseau est fermé au public et permet de sécuriser ce matériel comme faisant partie d'un réseau local sans limite d'accès au contenu web ou aux échanges possibles via internet.

Kirébos est destinée à la restriction des émetteurs du réseau, le serveur et les prises CPL, la domotique 5G.

Le programme cible les connexions entrantes et sortantes, surveille les flux du serveur afin de pouvoir exclure ou bloquer toute tentative de connexion intrusive. Une émission de rapport fait état de la consommation de données et collecte les adresses IP et Mac tentant de s'introduire de manière directe ou indirecte comme par exemple le placement ou l'installation d'un cookies renvoyant des données afin d'émettre un signal.

Les accès non-reconnus sont ensuite bloqués s'ils ne sont pas enregistrés comme faisant partie du réseau de l'infrastructure.

L'application :
Une icône de bureau (Desktop) permet un accès direct. L'application est bloquée en écriture et demande la reconnaissance de l'administrateur par un mot de passe crypté.

Le programme se présente sous la forme d'une fenêtre comprenant :

Un bouton « Déployer » permettant d'installer le module intégré au serveur.

Un bouton « Exporter le rapport » comprenant l'état du flux selon l'opérateur, les exemplaires des valeurs de l'application de l'opérateur, les données réelles collectées par le serveur, les adresses IP et Mac.

Un menu Etat du réseau, Données réseau et Collecte des connexions.
Un sous-menu fait état des graphiques de connexions grâce aux données renvoyées par le compte de l'opérateur afin d'établir un comparatif à différencier des flux du serveur.

Un sous-menu d'interrogation de mise à niveau des mises à jour du serveur et fait état des connexions (Dashboard Journalier, semestriel, mensuel et annuel) dans la même fenêtre.

Dans le dernier sous-menu se trouve les adresses bloquées ainsi que la collecte des adresses IP et Mac. Une boîte permet de passer les adresses bloquées à un accès validé tout comme pour un pare-feu.

Module de contrôle (traqueur) :
Un traqueur placé par l'application dans le serveur renvoie les données ainsi que le rapport à l'application de bureau. Celui-ci est bloqué en lecture et protégé par un mot de passe afin d'en sécuriser la fiabilité. Le traqueur suit les flux de données en temps-réel et prends les valeurs, stocke et renvoie son rapport dès la connexion au programme de surveillance disponible.

Le module de contrôle possède une image mémoire afin d'enregistrer et émettre le rapport mais c'est l'application de bureau et la mémoire de l'ordinateur de l'administratrice ou de l'administrateur qui entre le ou les rapports dans un dossier sécurisé crypté et protégé en lecture et en écriture afin d'en conserver l'intégrité.