Cible de sécurité Ého.Link

Contenu

Ce document décrit la solution Ého.Link ainsi que ses fonctions de sécurité implémentées pour protéger ses biens sensibles des menaces identifiées.

Référence : 2024_05_07_EHOLINK_CS_V2.5

CE DOCUMENT EST LA PROPRIÉTÉ DE ÉHO.LINK ET NE PEUT ÊTRE REPRODUIT OU COMMUNIQUÉ SANS AUTORISATION ÉCRITE
© ÉHO.LINK – 2024, Tous droits réservés

Révision	Date	Auteur	Commentaire
0.5	06/11/2019	Robin Milles	Version initiale
0.6	02/12/2019	Gilles Mareau	Relecture
0.7	06/01/2020	Robin Milles	Version finale
0.8	09/01/2020	Samantha Matchett	Relecture
1.0	10/01/2020	Sébastien Debosque	Approbation
1.3	23/04/2021	Robin Milles	Nouvelle version
1.4	27/04/2021	Robin Milles	Précisions
1.5	27/05/2021	Robin Milles	Corrections
1.6	17/09/2021	Gilles Mareau	Mise à jour versions
1.7	27/10/2021	Gilles Mareau / Robin Milles	Mises à jour : précisions, fonction de sécurité, version firmware sonde
2.0	10/02/2022	Gilles Mareau / Robin Milles	Mise à jour : précisions, détails, versions
2.1	20/10/2022	Gilles Mareau / Robin Milles	Mises à jour réévaluation suite RTE 02/2022
2.2	20/01/2023	Gilles Mareau / Robin Milles	Mise à jour versions logicielles
2.3	24/07/2023	Gilles Mareau / Robin Milles	Mise à jour versions logicielles
2.4	02/05/2024	Gilles Mareau / Robin Milles	Mise à jour documentaire
2.5	07/05/2024	Gilles Mareau / Robin Milles	Mise à jour documentaire

CE DOCUMENT EST LA PROPRIÉTÉ DE ÉHO.LINK ET NE PEUT ÊTRE REPRODUIT OU COMMUNIQUÉ SANS AUTORISATION ÉCRITE
© ÉHO.LINK - 2024, Tous droits réservés

CE DOCUMENT EST LA PROPRIÉTÉ DE ÉHO.LINK ET NE PEUT ÊTRE REPRODUIT OU COMMUNIQUÉ SANS AUTORISATION ÉCRITE
© ÉHO.LINK - 2024, Tous droits réservés

1. Identification de la cible

Cette cible de sécurité a été élaborée en vue d'une évaluation Certification Sécurité de Premier Niveau (CSPN).

Éditeur	Ého.Link
Site de l'éditeur	https://www.eho.link/
Nom du produit à évaluer	Logiciel single tenant Ého.Link en tant que service (SaaS) En hébergement Cloud privé sur socle PaaS
Référence	EHOLINK
Version soumise à évaluation	Hardware Ého.Box EHOLINK_A2.2 avec software version 22.02.0.5 Eho.my version 24.03.0.1 Eho.cloud version 22.03.1.1
Catégorie de produit	Administration et supervision de la sécurité

2. Description du produit

2.1 Description générale

Ého.Link est une solution qui a pour but de contrôler les accès du Système d'Information, d'en détecter les équipements connectés, d'analyser l'activité sur le réseau privé, d'administrer l'usage d'internet, de mettre en conformité le responsable légal et les utilisateurs sur la réglementation en vigueur dans leur pays, le stockage sécurisé des données dans un cloud personnel avec des serveurs localisés dans le pays du client.

La solution est accessible aux TPE comme aux entreprises de 250 personnes via un boîtier branché sur le réseau après le routeur qui nécessite une authentification sur une page web par utilisateur et permet en plus l'accès à un cloud personnel, lui-même accessible depuis l'extérieur via l'authentification sur la même page web.

La solution Ého.Link est composée des éléments suivants :

- Ého.Box :

Est le boîtier conçu par Ého.Link, il se positionne en coupure des accès internes et externes du SI, et il est le support du système de détection d'intrusions réseau et de contrôle d'accès. Il dispose d'une fonction de mise à jour automatique de son firmware ainsi que de la base de signatures de l'IDS, fonctionne avec un système d'exploitation propriétaire basé sur un noyau Linux modifié, lui-même fonctionnant sur une plateforme ARM Marvell ARMADA.

- Ého.Cloud :

Est le service de cloud personnel pour chaque utilisateur proposé par Ého.Link.

CE DOCUMENT EST LA PROPRIÉTÉ DE ÉHO.LINK ET NE PEUT ÊTRE REPRODUIT OU COMMUNIQUÉ SANS AUTORISATION ÉCRITE
© ÉHO.LINK - 2024, Tous droits réservés

- Ého.My :

Est le portail web sur lequel il faut s'authentifier pour accéder à internet et à son cloud si on est connecté sur une Ého.Box ou pour accéder uniquement à son cloud si on est connecté directement à internet.

L'utilisation de la solution Ého.Link ne nécessite pas l'installation de logiciel client ou de configuration particulière sur les périphériques utilisateur.

Indépendance totale du produit

- Aucune dépendance vis à vis du fournisseur d'accès : ne gère pas l'accès internet des clients.

- Aucune dépendance matérielle vis à vis d'aucun constructeur : conception propriétaire d'Ého.Box.

- Aucune licence liée : pas de dépendance vis à vis d'un éditeur de logiciel : aucune licence commerciale.

- Aucun protocole propriétaire tiers

CE DOCUMENT EST LA PROPRIÉTÉ DE ÉHO.LINK ET NE PEUT ÊTRE REPRODUIT OU COMMUNIQUÉ SANS AUTORISATION ÉCRITE
© ÉHO.LINK - 2024, Tous droits réservés

2.2 Principales caractéristiques

Administrer l'usage d'internet :
Synthèse de l'ensemble des statistiques collectées, stockées dans une base de données, pouvant être analysées d'un niveau macro (société) à micro (utilisateur) :

- Consommation de la bande passante
- Sites visités : classement par utilisateurs les plus consommateurs d'internet, classement des sites internet les plus visités, etc.
- Horaires et durée de connexion
- Identification et vérification de l'ensemble des sites Internet entrants et sortants

Pouvant être consultée sur l'interface web, accessible de façon sécurisée (HTTPS), qui met à disposition un tableau de bord avec une vue générale sur les éléments précédemment cités.

Détecter les équipements connectés :
Découverte de l'ensemble des équipements connectés au sous réseau et notification de toute connexion d'un nouvel équipement

Contrôler les accès au SI :
Gestion des autorisations des équipements connectés au réseau interne, des utilisateurs et des protocoles.
Ouverture / fermeture de l'accès par horodatage

Mettre en conformité le responsable légal et les utilisateurs sur la réglementation :
Génération automatisée de la charte informatique, qui permet :

- La protection du patrimoine informationnel de l'entreprise
- La définition des responsabilités de chaque utilisateur et des règles internes d'utilisation, notamment la séparation entre les éléments professionnels et privés des salariés
- La mise en conformité légale des opérations de cybersurveillance et de cyber-protection des salariés ainsi que la collecte licite de preuves électroniques nécessaires en cas de contentieux

Sensibilisation et aide à la mise en conformité RGPD

Analyser l'activité réseau privé :
Se base sur un système de détection d'intrusion réseau (NIDS = Network Based Intrusion Detection System) proposant une analyse de flux réseau et des remontées d'alertes.
Capte l'intégralité de l'information entrante et sortante : capture et traitement full stack (L1 à 7)
Pont logiciel en local basé sur un moteur de traitement de paquets réseau effectuant une inspection profonde (Deep Packet Inspection) en temps réel, en 3 étapes :

- Capture des paquets réseau
- Classement par flux, regroupant les paquets réseaux pour former les flux de discussion entre les différents hôtes
- Inspection profonde des paquets

CE DOCUMENT EST LA PROPRIÉTÉ DE ÉHO.LINK ET NE PEUT ÊTRE REPRODUIT OU COMMUNIQUÉ SANS AUTORISATION ÉCRITE
© ÉHO.LINK - 2024, Tous droits réservés

L'IDS propose les fonctionnalités suivantes :

- La détection d'intrusion basée sur l'utilisation de signatures, qui se mettent à jour automatiquement.
- Des mécanismes de réponse faisant suite à la détection d'un trafic anormal tels que :
  - Le blocage des flux par l'IDS positionné en coupure.
  - La remontée d'alertes sur le portail Ého.My pour autoriser les flux bloqués si faux positif.

L'analyse se fait de manière passive et transparente, c'est-à-dire qu'elle n'altère pas les paquets réseaux que l'IDS traite.

L'IDS génère des journaux détaillés qui sauvegardent les différents événements observés. Ces journaux peuvent s'avérer utiles lors de la phase de diagnostic réalisée lorsqu'une attaque est détectée (analyse post mortem).

Figure 1 : Tableau de Bord

CE DOCUMENT EST LA PROPRIÉTÉ DE ÉHO.LINK ET NE PEUT ÊTRE REPRODUIT OU COMMUNIQUÉ SANS AUTORISATION ÉCRITE
© ÉHO.LINK - 2024, Tous droits réservés

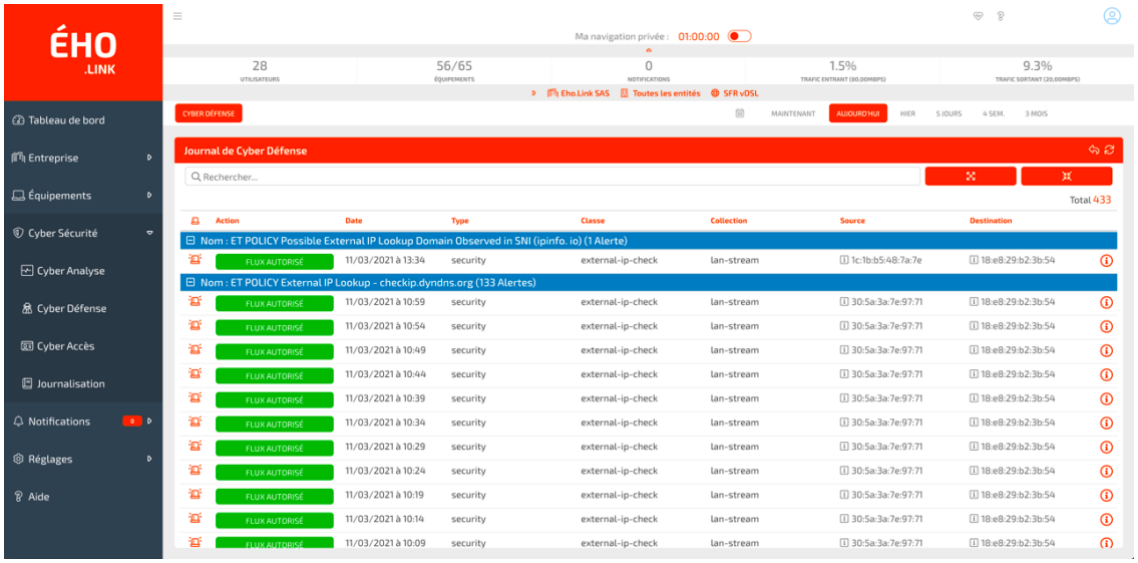

Figure 2 : Onglet Cyberdéfense

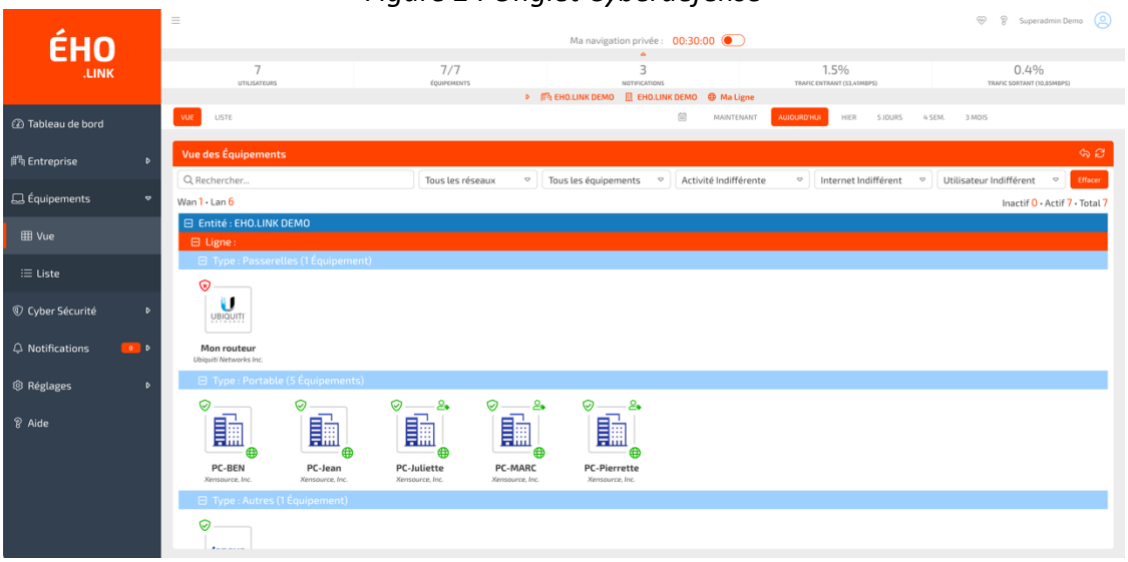

Figure 3 : Onglet équipements

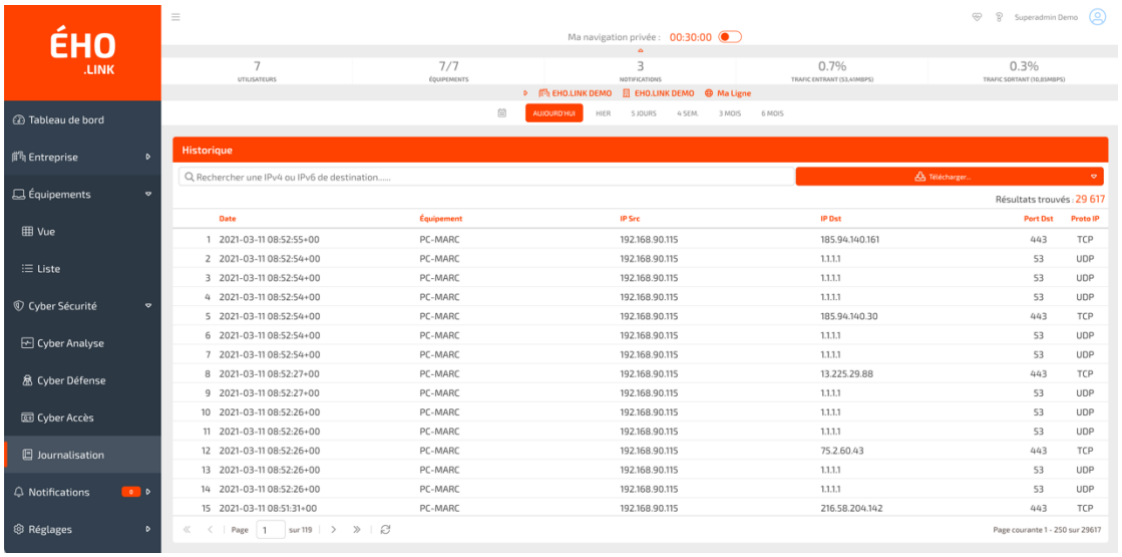

Figure 4 : Onglet journalisation

CE DOCUMENT EST LA PROPRIÉTÉ DE ÉHO.LINK ET NE PEUT ÊTRE REPRODUIT OU COMMUNIQUÉ SANS AUTORISATION ÉCRITE
© ÉHO.LINK - 2024, Tous droits réservés

Figure 5 : Ého.Box

Sonde Ého.Link:

Carte	Design 100% interne
CPU	SoC Marvell Armada 7040 (Quad core – ARM64 1.4Ghz) - Secure boot
RAM	2Go DDR4, pistes d'adresses enfouies
Stockage	8Go eMMC HS200 - Chiffré
TPM	STMicroelectronics ST33TPHF2ESPI mode TPM 2.0 certifié CC EAL4+
Réseaux	Deux ports Ethernet 1Gb/s avec Bypass matériel
Connectique	Port USB3.1 (USB-C)
Boitier	Boitier métal anti feu
Alimentation	Alimentation 12v 3A
Autre	Ventilation contrôlée
	Ecran tactile couleur
	Beeper

Cloud privé basé en France :

Localisation dans un datacenter Tiers 4 (Interxion Marseille MRS2)
Location de baie bare-metal (aucun intervenant extérieur admis),
Adduction réseau sur opérateur Tiers 1 (ASN 211997)
Disques dur chiffrés FIPS140
Détection d'ouverture de porte, enregistrement des ouvertures (Webcam)

CE DOCUMENT EST LA PROPRIÉTÉ DE ÉHO.LINK ET NE PEUT ÊTRE REPRODUIT OU COMMUNIQUÉ SANS AUTORISATION ÉCRITE
© ÉHO.LINK - 2024, Tous droits réservés

2.3 Description de l'environnement technique de fonctionnement

Le produit se branche en coupure entre le réseau à sécuriser et le réseau extérieur, il permet la connexion avec tous types de périphériques réseaux. (cf. Figure 6)

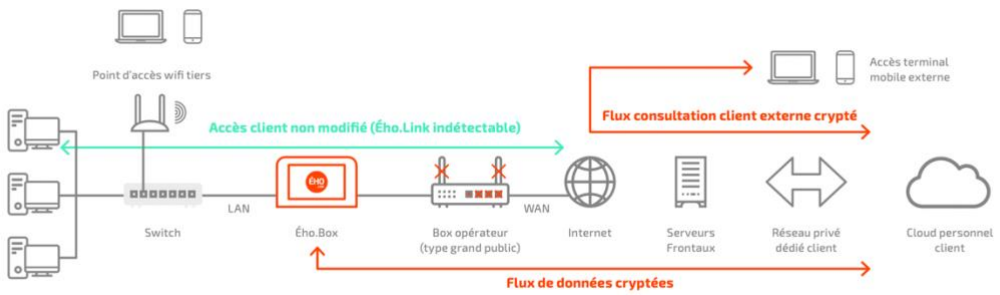

Figure 6 : Exemple d'environnement

Il s'intègre dans un réseau IPv4 ou IPv6 et ne nécessite aucune modification sur les postes clients ou sur les équipements à protéger.

CE DOCUMENT EST LA PROPRIÉTÉ DE ÉHO.LINK ET NE PEUT ÊTRE REPRODUIT OU COMMUNIQUÉ SANS AUTORISATION ÉCRITE
© ÉHO.LINK - 2024, Tous droits réservés

2.4 Architecture

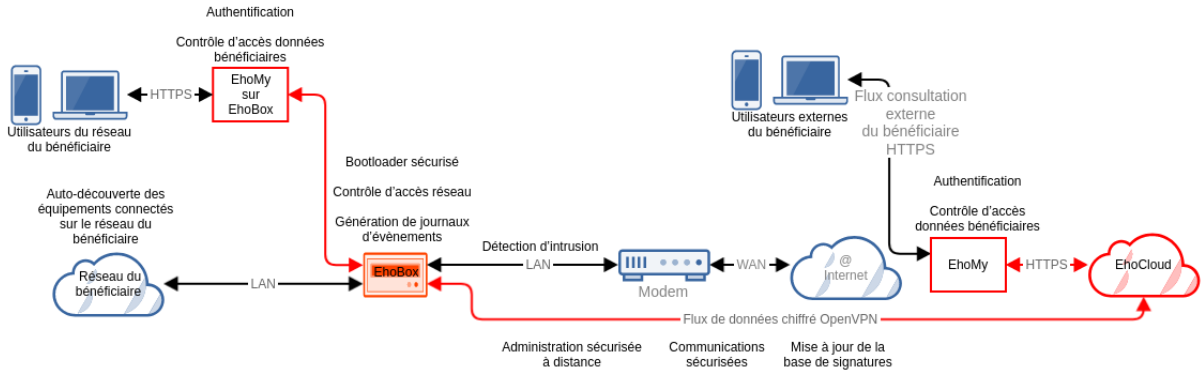

Figure 7 : Schéma d'architecture

Échanges Ého.Box/Ého.Cloud :

L'Ého.Box et Ého.Cloud communiquent via un tunnel OpenVPN en établissant une connexion TLS avec authentification mutuelle (le certificat d'Ého.Box est valide pour Ého.Cloud et inversement)

Échanges Ého.My/Ého.Cloud :

Ého.My et Ého.Cloud communiquent via une connexion HTTPS avec authentification mutuelle (le certificat d'Ého.My est valide pour Ého.Cloud et inversement)

CE DOCUMENT EST LA PROPRIÉTÉ DE ÉHO.LINK ET NE PEUT ÊTRE REPRODUIT OU COMMUNIQUÉ SANS AUTORISATION ÉCRITE
© ÉHO.LINK - 2024, Tous droits réservés

2.6 Périmètre d'évaluation

Les fonctions de sécurité suivantes font partie du périmètre de l'évaluation

Ého.Box

- Bootloader sécurisé
- Filtrage réseau
- Génération de journaux d'évènements
- Administration sécurisée à distance
- Communications sécurisées
- Mise à jour de la base de signatures
- Mise à jour du firmware
- Protection des clés

Ého.Cloud

- Communications sécurisées
- Authentification
- Protection des clés

Ého.My

- Authentification
- Contrôle d'accès données globales bénéficiaires
- Protection des clés

Les fonctions de sécurité suivantes ne font pas partie du périmètre d'évaluation :

- La détection d'intrusion en tant que mécanisme ne fait pas partie du périmètre d'évaluation
- Auto-découverte des équipements connectés sur le réseau du bénéficiaire
- Contrôle d'accès réseau

Liste des services actifs sur les composants

- Service web de Status sur l'Ého.Box

Liste des dépendances du produit (versions au 24/07/2023) :

Pour Ého.Cloud

Lxd	5.0.2
Debian	12.1
Kernel linux	6.1.38-1
Nginx	1.24.0
Php	8.1.21
Openssl	3.0.9
Openssh-server	9.3p2
Postgresql	15.3
Openvpn	2.6.5

CE DOCUMENT EST LA PROPRIÉTÉ DE ÉHO.LINK ET NE PEUT ÊTRE REPRODUIT OU COMMUNIQUÉ SANS AUTORISATION ÉCRITE
© ÉHO.LINK - 2024, Tous droits réservés

Pour Ého.My

Lxd	5.0.2
Debian	12.1
Kernel linux	6.1.38-1
Nginx	1.24.0
Php	8.1.21
Openssl	3.0.9
Openssh-server	9.3p2
Redis-server	7.0.12

Pour Ého.Box (22.02.0.5)

U-Boot	v2023.07.02
Linux kernel	5.10.186
openssl	3.0.9
pkix-ssh	14.1.1
tpm2-tools	5.5
tpm2-tss	4.0.1
eholink-pkcs11	22.02.0.4
pkcs11-helper	1.29
libp11	0.4.12
p11-kit	0.25.0
cryptsetup	2.6.1
rhash	1.4.4
openvpn	2.6.5
GNU libc	2.37
busybox	1.36.1
curl, libcurl	8.2.0
ca-bundle	20230311
nginx	1.24.0
Php	8.1.21
TPM STMicroelectronics	ST33TPHF2ESPI mode TPM 2.0 certifié CC EAL4+ (ST33HTPH2E32AAF1 en fw 0x49.0x14)
minijail	V18

Pour Eho.PKI

Debian	12.1
Kernel linux	6.1.38-1
Openssl	3.0.9

Les mises à jour sont effectuées mensuellement à partir d'un miroir local sauf pour les mises à jour de sécurité et vulnérabilités critiques exploitables qui sont effectuées dès que la mise à jour est disponible.

CE DOCUMENT EST LA PROPRIÉTÉ DE ÉHO.LINK ET NE PEUT ÊTRE REPRODUIT OU COMMUNIQUÉ SANS AUTORISATION ÉCRITE
© ÉHO.LINK - 2024, Tous droits réservés

TPM STMicroelectronics :
ST33TPHF2ESPI mode TPM 2.0 certifié CC EAL4+ en firmware 49.14.
CC EAL4+ : https://www.ssi.gouv.fr/uploads/2019/11/anssi-cc-2019_53fr.pdf
FIPS140-2 : https://csrc.nist.gov/CSRC/media/projects/cryptographic-module-validation-program/documents/security-policies/140sp3681.pdf

Nitrokey HSM2 :
Utilise une Cardcontact smartcard-HSM sim 4k :
https://www.smartcard-hsm.com/docs/sc-hsm-4k-datasheet.pdf
Certificat CC EAL5+ JCOP3 P60 :
https://www.commoncriteriaportal.org/files/epfiles/[CR]%20NSCIB-CC-98209-CR3.pdf
https://www.commoncriteriaportal.org/files/epfiles/[ST-Lite]%20ST-Lite_JCOP3_P60_v3.8.pdf
Version Nitrokey HSM2 / Cardcontact : 3.5

CE DOCUMENT EST LA PROPRIÉTÉ DE ÉHO.LINK ET NE PEUT ÊTRE REPRODUIT OU COMMUNIQUÉ SANS AUTORISATION ÉCRITE
© ÉHO.LINK - 2024, Tous droits réservés

2.7 Description des rôles

Les rôles de la solution sont les suivants :

Un administrateur de l'infrastructure technique qui :

- A un accès total au boîtier et au cloud en cas de problème
- Gère les comptes administrateurs
- Est le fournisseur du socle

Un administrateur système qui :

- Crée les conteneurs pour le cloud du client
- A en charge la maintenance du cloud
- Gère le compte Administrateur métier ou compte utilisateur final
- Est le fournisseur du socle

Un installateur qui :

- A en charge l'installation du boîtier
- Aide au paramétrage de la solution
- Est l'intégrateur

Un administrateur métier qui :

- Dispose de l'accès total aux informations concernant les utilisateurs de sa société
- Gère les comptes utilisateurs
- Gère les autorisations des périphériques connectés
- Gère la configuration du contrôle d'accès
- Est responsable de la mise en conformité légale
- Reçoit les notifications lors de la détection d'intrusions
- Est le bénéficiaire

Un utilisateur final qui :

- Dispose d'un accès limité uniquement aux informations le concernant sur l'interface web.
- Peut obtenir des droits de la part de l'administrateur métier pour effectuer certaines taches de celui-ci.
- Est le bénéficiaire

CE DOCUMENT EST LA PROPRIÉTÉ DE ÉHO.LINK ET NE PEUT ÊTRE REPRODUIT OU COMMUNIQUÉ SANS AUTORISATION ÉCRITE
© ÉHO.LINK - 2024, Tous droits réservés

Utilisateur final	Utilisation métier
Administrateur métier	Paramétrage métier
Administrateur système	Logiciel et données Intergiciels et autres logiciels de base Système d'exploitation Ressources virtualisées
Administrateur technique de l'infrastructure	Couche de virtualisation Machine physique, réseau et stockage
Officier de sécurité	Sécurité des locaux et du personnel

Rôles tenus par le bénéficiaire
Rôles tenus par le fournisseur de socle

Eho Link est le fournisseur du socle et le développeur de la solution.

CE DOCUMENT EST LA PROPRIÉTÉ DE ÉHO.LINK ET NE PEUT ÊTRE REPRODUIT OU COMMUNIQUÉ SANS AUTORISATION ÉCRITE
© ÉHO.LINK - 2024, Tous droits réservés

2.8 Profil des attaquants

Les attaquants potentiels sont des attaquants externes (des personnes extérieures au réseau protégé).
Les attaques peuvent être menées à partir de l'externe ou de l'interne (si une machine interne a été compromise par un attaquant externe).

On distingue les profils suivants :

- Attaquants hors bénéficiaires qui tentent de modifier la configuration d'une ou plusieurs TOE via Ého.My ou alors de s'introduire dans le réseau du bénéficiaire au travers de l'Ého.Box

- Attaquants intra-bénéficiaires qui tentent de modifier la configuration d'une TOE ou d'obtenir des droits supérieurs sur Ého.My.

- Attaquants extra-bénéficiaires qui tentent au travers de Ého.My d'obtenir des privilèges sur la configuration d'un autre bénéficiaire.

CE DOCUMENT EST LA PROPRIÉTÉ DE ÉHO.LINK ET NE PEUT ÊTRE REPRODUIT OU COMMUNIQUÉ SANS AUTORISATION ÉCRITE
© ÉHO.LINK - 2024, Tous droits réservés

2.9 Description des hypothèses sur l'environnement

Hypothèses concernant la partie cloud :

H.ADMINTECH_CONFIANCE
Les administrateurs de l'infrastructure technique et système sont des personnes considérées comme non hostiles. Ils sont formés pour administrer et configurer les produits. Ils suivent les procédures d'administration.

H.INSTALLATEUR_CONFIANCE
Les installateurs sont des personnes considérées comme non hostiles. Ils sont formés pour installer les produits. Ils suivent les procédures d'installation.

H.ADMINMETIER_CONFIANCE
L'administrateur métier est considéré comme non hostile et de confiance vis-à-vis de son périmètre d'intervention.

H.UTILISATEUR_CONFIANCE
L'utilisateur final qui a des droits sur la TOE est de confiance dans son périmètre.

H.TACHE_UTILISATEUR
L'utilisateur final suit les règles ANSSI pour construire un mot de passe robuste et s'assure que ce mot de passe n'est pas partagé avec d'autres utilisateurs.

H.TACHE_ADMIN_METIER
L'administrateur métier doit configurer la TOE suivant les procédures qui lui sont données et consulter régulièrement les données de journalisation.

H.TACHE_INSTALLATEUR
L'installateur doit réinitialiser l'Eho.Box dans la version d'usine pour ne contenir aucune donnée clients, et vérifier que le produit est installé dans un local sécurisé et accessible uniquement par les administrateurs métier.

H.TACHE_ADMIN_INFRA_PHY
L'administrateur d'infrastructure technique doit vérifier que les interfaces d'administration des équipements sont accessibles uniquement aux personnels habilités.

H.TACHE_ADMIN_INFRA_PATCH
L'administrateur d'infrastructure technique doit vérifier que l'OS ainsi que les logiciels sont à jour des patches de sécurité.

H.TACHE_ADMIN_INFRA_CRYPTO
L'administrateur d'infrastructure technique doit générer les clés sur la PKI et par GlobalSign en conformité avec le GMC et les transmettre aux différents éléments (Eho.Box, Eho.Cloud, Eho.My) de manière sécurisée.

CE DOCUMENT EST LA PROPRIÉTÉ DE ÉHO.LINK ET NE PEUT ÊTRE REPRODUIT OU COMMUNIQUÉ SANS AUTORISATION ÉCRITE
© ÉHO.LINK - 2024, Tous droits réservés

H.CLOUD_CONFIANCE
La solution cloud est installée dans un cloud privé basé en France, les installateurs et exploitants de cette solution sont considérés comme non hostiles et de confiance vis-à-vis de leur périmètre d'intervention.

Hypothèses concernant la partie Eho.Box :

H.COUPURE
Le boîtier est installé conformément à la politique d'interconnexion des réseaux en vigueur et est le seul point de passage entre les différents réseaux sur lesquels il faut appliquer la politique de contrôle d'accès.

H.CPU
Le système de Secureboot fourni par Marvell est considéré comme fiable et fourni l'intégrité et l'authenticité des signatures des firmwares et la confidentialité des clés de chiffrement du firmware

H.TPM
Le bon fonctionnement du TPM est garanti par sa certification
(ST33TPHF2ESPI mode TPM 2.0 certifié CC EAL4+)

H.HSM
Le bon fonctionnement des clés HSM est garanti par leurs certifications
(Cardcontact smartcard-HSM sim 4k JCOP3 P60 certifié CC EAL 5+)

H.LAN_INTERNE
Il est supposé que le bénéficiaire assure la sécurité du réseau interne connecté à la ToE en particulier il garantit l'identification des flux interne.

CE DOCUMENT EST LA PROPRIÉTÉ DE ÉHO.LINK ET NE PEUT ÊTRE REPRODUIT OU COMMUNIQUÉ SANS AUTORISATION ÉCRITE
© ÉHO.LINK - 2024, Tous droits réservés

3. Description des biens sensibles

3.1 Description des biens sensibles de l'environnement de la TOE

Flux Bénéficiaires internet (bien sensible de l'utilisateur final de la TOE)
Il s'agit des flux de communications d'un bénéficiaire quand il utilise son réseau d'accès internet. Ces flux sont filtrés par l'Ého.Box. Besoin de sécurité : intégrité*.

Flux Bénéficiaires de configuration (bien sensible de l'administrateur métier de la TOE)
Il s'agit des flux de communication entre un administrateur métier et le portail Ého.My, lui permettant d'administrer et de configurer les Ého.Box. Besoin de sécurité : confidentialité et intégrité

Flux Ého.Box/Ého.Cloud (bien sensible de la TOE elle-même)
Il s'agit des flux de communication entre une Ého.Box et le Ého.Cloud. Besoin de sécurité : confidentialité et intégrité

Flux Ého.My/Ého.Cloud (bien sensible de la TOE elle-même)
Il s'agit des flux de communication entre une Ého.My et le Ého.Cloud. Besoin de sécurité : confidentialité et intégrité

Base d'identification utilisateurs (bien sensible de l'utilisateur final de la TOE)
Cette base contient les identifiants et les moyens d'assurer l'authentification des utilisateurs du SI sur Ého.My. La base est stockée sur Ého.Cloud (une base par bénéficiaire). Besoin de sécurité : confidentialité et intégrité.

** L'Ého.Box ne modifie pas les flux utilisateurs et donc la confidentialité et l'authenticité dépendent de l'utilisateur*

3.2 Description des biens sensibles de la TOE

Firmware d'Ého.Box (bien sensible de la TOE elle-même)
Afin d'assurer correctement ses fonctions, le firmware d'Ého.Box doit être intègre et authentique.

Politique de filtrage réseaux (bien sensible de l'administrateur métier de la TOE)
Contient toutes les politiques de filtrage des flux. La politique est définie via Ého.My, puis stockée sur Ého.Cloud ainsi que sur l'Ého.Box.
La politique doit être intègre.

Données statistiques des bénéficiaires (bien sensible de la TOE elle-même)
Stocke les informations de trafic des bénéficiaires sur Ého.Cloud. Elle doit être confidentielle.

CE DOCUMENT EST LA PROPRIÉTÉ DE ÉHO.LINK ET NE PEUT ÊTRE REPRODUIT OU COMMUNIQUÉ SANS AUTORISATION ÉCRITE
© ÉHO.LINK - 2024, Tous droits réservés

La base de signatures (bien sensible de la TOE elle-même)
La méthode de détection d'intrusion de l'IDS est basée sur l'utilisation d'une base de signatures qui est mise à jour périodiquement de manière centralisée sur Ého.Cloud puis déployée sur les Ého.Box. Cette base doit être intègre.

Les journaux d'audits et d'alertes (bien sensible de la TOE elle-même)
Des notifications de détection d'intrusions sont remontées par l'IDS afin d'être traitées par le représentant légal et des journaux sont générés pour des pistes d'audit qui sont stockés localement dans l'Ého.Box puis transmis à Ého.Cloud dans une base de données. Besoin de sécurité : confidentialité et intégrité.

Clés Ého.Box (bien sensible de la TOE elle-même)
En ce qui concerne les clés d'authentification :

- KAK SB key pair
  Besoin de sécurité : confidentialité, intégrité, authenticité

- CSK SB key pair
  Besoin de sécurité : confidentialité, intégrité, authenticité

- FW SB key pair
  Besoin de sécurité : confidentialité, intégrité, authenticité

- FW UP SIGN key pair
  Besoin de sécurité : confidentialité, intégrité, authenticité

- FW UP CRYPT key pair
  Besoin de sécurité : confidentialité, intégrité, authenticité

En ce qui concerne les clés de chiffrement :

- AES SB key
  Besoin de sécurité : confidentialité, intégrité, authenticité

- AES UP key
  Besoin de sécurité : confidentialité, intégrité, authenticité

- LUKS TPM key
  Besoin de sécurité : confidentialité, intégrité, authenticité

En ce qui concerne les clés d'échange avec Ého.Cloud :

- BOX_FACTORY
  Besoin de sécurité : confidentialité, intégrité, authenticité

- BOX_CUSTOMER
  Besoin de sécurité : confidentialité, intégrité, authenticité

CE DOCUMENT EST LA PROPRIÉTÉ DE ÉHO.LINK ET NE PEUT ÊTRE REPRODUIT OU COMMUNIQUÉ SANS AUTORISATION ÉCRITE
© ÉHO.LINK - 2024, Tous droits réservés

En ce qui concerne les clés d'échange avec Status :

- STATUS
  Besoin de sécurité : confidentialité, intégrité, authenticité

Clés Ého.Cloud (bien sensible de la TOE elle-même)

- CONTAINER_CUSTOMER
  Besoin de sécurité : confidentialité, intégrité, authenticité

- CONTAINER_SERVICE
  Besoin de sécurité : confidentialité, intégrité, authenticité

Clés Ého.My (bien sensible de la TOE elle-même)

- SERVER
  Besoin de sécurité : confidentialité, intégrité, authenticité

- PUBLIC
  Besoin de sécurité : confidentialité, intégrité, authenticité

Clés pour l'administration SSH à distance des Ého.Box (bien sensible de la TOE elle-même)

- Clé RSA 4096
  Besoin de sécurité : confidentialité, intégrité, authenticité

CE DOCUMENT EST LA PROPRIÉTÉ DE ÉHO.LINK ET NE PEUT ÊTRE REPRODUIT OU COMMUNIQUÉ SANS AUTORISATION ÉCRITE
© ÉHO.LINK - 2024, Tous droits réservés

Biens sensibles	Disponibilité	Confidentialité	Intégrité	Authenticité
Flux Bénéficiaires internet			X	
Flux Bénéficiaires de configuration		X	X	
Flux Ého.Box/Ého.Cloud		X	X	
Flux Ého.My/Ého.Cloud		X	X	
Base d'identification utilisateurs		X	X	
Firmware d'Ého.Box			X	X
Politique de filtrage réseaux			X	
Données statistiques des bénéficiaires		X		
Base de signatures			X	
Les journaux d'audits et d'alertes		X	X	
Clés Ého.Box		X	X	X
Clés Ého.Cloud		X	X	X
Clés Ého.My		X	X	X
Clés pour l'administration SSH à distance des Ého.Box		X	X	X

4. Description des menaces

Corruption du firmware

Un attaquant (hors, extra ou intra bénéficiaire) parvient à injecter et faire exécuter un firmware corrompu sur le boîtier. L'injection de code peut être temporaire ou permanente et ceci inclut donc toute exécution de code non prévue ou non autorisée.
Un attaquant (hors, extra ou intra bénéficiaire) peut également réussir à substituer une mise à jour corrompue à une mise à jour légitime.

Contournement de la politique de filtrage

Un attaquant (hors, extra ou intra bénéficiaire) parvient à contourner la politique de filtrage d'accès implémentée sur l'Ého.Box et ainsi empêcher un flux légitime ou permettre un flux illégitime de transiter. Il peut également tenter de désactiver la politique ou de modifier les flux des bénéficiaires.

Accès illicite hors bénéficiaire

Un attaquant hors bénéficiaire tente d'accéder de manière illicite à Ého.Cloud pour consulter et/ou modifier illicitement des données sensibles (politique d'accès, données statistiques, mot de passe des bénéficiaires, journaux, …).

CE DOCUMENT EST LA PROPRIÉTÉ DE ÉHO.LINK ET NE PEUT ÊTRE REPRODUIT OU COMMUNIQUÉ SANS AUTORISATION ÉCRITE
© ÉHO.LINK - 2024, Tous droits réservés

Accès illicite intra bénéficiaire

Un attaquant intra bénéficiaire tente d'accéder de manière illicite à Ého.My pour consulter et/ou modifier illicitement des données sensibles intra-bénéficiaire (via la définition de la politique de contrôle ou les statistiques)

Accès illicite extra bénéficiaire

Un attaquant extra bénéficiaire tente d'accéder de manière illicite à Ého.My pour consulter et/ou modifier illicitement des données sensibles d'un autre bénéficiaire (via la définition de la politique de contrôle ou les statistiques)

Accès illicite Ého.Box

Un attaquant (hors, extra ou intra bénéficiaire) tente d'accéder de manière illicite à Ého.Box pour modifier illicitement le fonctionnement de l'Ého.Box

Élévation de privilège

Un utilisateur final d'un bénéficiaire tente d'obtenir les droits d'un administrateur métiers via Ého.My

Corruption des mises à jour IDS

Un attaquant (hors, extra ou intra bénéficiaire) tente d'exploiter une faille dans le processus de mises à jour de la base de signatures de l'IDS lorsque cette opération n'est pas régulière (données de signature obsolètes) ou réalisée à partir de données de signature de mauvaise qualité (ne répertoriant pas toutes les signatures publiques).

Accès aux journaux

Un attaquant (hors, extra ou intra bénéficiaire) tente d'accéder aux journaux voire de les modifier illicitement.

Corruption des flux

Un attaquant (hors, extra ou intra bénéficiaire) tenter d'intercepter les communications entre les différents composants de la TOE (Ého.Box, Ého.My, Ého.Cloud) afin de consulter/modifier le contenu.

Vol de clés

Un attaquant (hors, extra ou intra bénéficiaire) tente de récupérer les clés stockées dans les différents composants de la TOE (Ého.Box, Ého.My, Ého.Cloud) afin mettre en défaut les mécanismes cryptographiques mis en œuvre par la TOE. Ceci permettant des interceptions de communication, des mises à jour illicites….

CE DOCUMENT EST LA PROPRIÉTÉ DE ÉHO.LINK ET NE PEUT ÊTRE REPRODUIT OU COMMUNIQUÉ SANS AUTORISATION ÉCRITE
© ÉHO.LINK - 2024, Tous droits réservés

5. Description des fonctions de sécurité du produit

Bootloader sécurisé

À chaque démarrage du boîtier, l'intégrité et l'authenticité du firmware est vérifiée grâce à sa signature stockée dans le bootloader, et sa confidentialité grâce au chiffrement (la clé est stockée dans le bootloader).

En ce qui concerne les clés d'authentification :

- KAK SB key pair (RSA-SSA-PSS 2048)
  - Phase : Secureboot (SoC bootRom vers bootloader)
  - Elle authentifie les headers du bootloader – U-boot (signature)

- CSK SB key pair (RSA-SSA-PSS 2048)
  - Phase : Secureboot (SoC bootRom vers bootloader)
  - Elle authentifie l'image du bootloader – U-boot (signature)

- FW SB key pair (RSA 2048)
  - Phase : Bootloader (bootloader vers firmware)
  - Elle authentifie le firmware Linux (FIT images) (signature)

En ce qui concerne les clés de chiffrement :

- AES SB key (AES 256 CBC)
  - Phase : Secureboot (SoC bootRom vers bootloader)
  - Elle déchiffre le bootloader U-boot (chiffrement image)

- LUKS TPM key (AES-XTS-PLAIN64, 2x 256 bits)
  - Phase : RootFS
  - Elle déchiffre le rootfs du firmware Linux (chiffrement)

CE DOCUMENT EST LA PROPRIÉTÉ DE ÉHO.LINK ET NE PEUT ÊTRE REPRODUIT OU COMMUNIQUÉ SANS AUTORISATION ÉCRITE
© ÉHO.LINK - 2024, Tous droits réservés

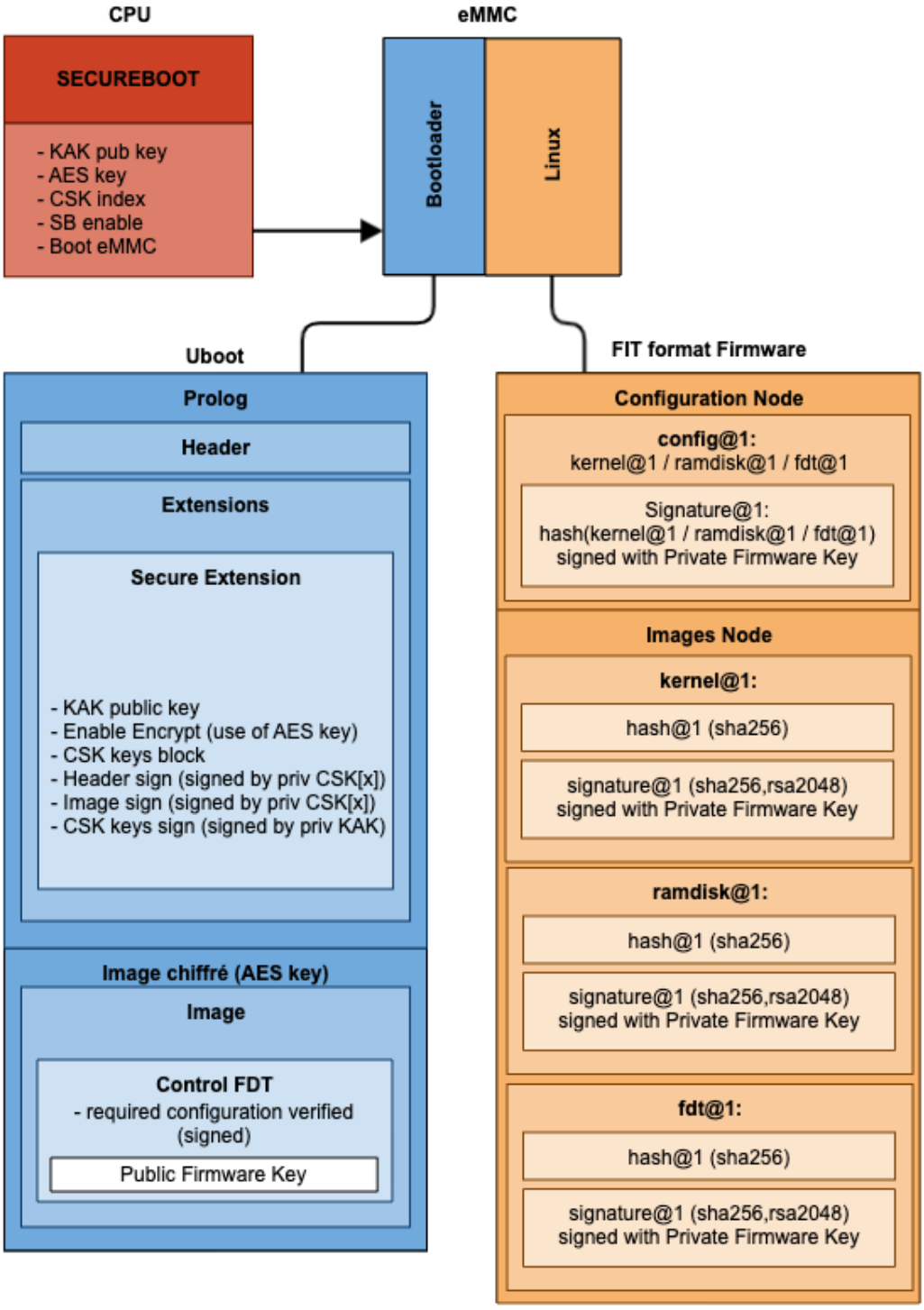

Figure 8 : Structure des différents composants

Mise à jour du firmware

L'Ého.Box est capable de se mettre à jour automatiquement pour corriger des failles de sécurité, le firmware est transmis via la communication sécurisée qui assure la confidentialité* avec authentification mutuelle, l'intégrité et l'authenticité du firmware sont vérifiées grâce à sa signature stockée (la clé publique FW UP SIGN est stockée dans l'image du firmware

CE DOCUMENT EST LA PROPRIÉTÉ DE ÉHO.LINK ET NE PEUT ÊTRE REPRODUIT OU COMMUNIQUÉ SANS AUTORISATION ÉCRITE
© ÉHO.LINK - 2024, Tous droits réservés

téléchargé). La clé AES UP, qui est transmise avec le firmware, est ensuite déchiffrée avec la clé publique FW UP CRYPT stockée dans la box et connue des boxs uniquement. Enfin le firmware est déchiffré avec la clé AES UP.

En ce qui concerne les clés d'authentification :

- FW UP SIGN key pair (RSA-SSA-PSS 4096)
  - Phase : Firmware
  - Elle authentifie le package de mise à jour firmware téléchargé (signature)

- FW UP CRYPT key pair (RSA 4096)
  - Phase : Firmware
  - Elle déchiffre le package de mise à jour firmware téléchargé

En ce qui concerne les clés de chiffrement :

- AES UP key (AES 256 CBC)
  - Phase : Firmware
  - Elle déchiffre l'image du firmware Linux téléchargé (chiffrement)

** La confidentialité n'est assurée que durant le transport, les paquets de firmware ne sont transmis que via le service de mise à jour et son accès est garanti par l'hypothèse H.ADMINTECH_CONFIANCE.*

CE DOCUMENT EST LA PROPRIÉTÉ DE ÉHO.LINK ET NE PEUT ÊTRE REPRODUIT OU COMMUNIQUÉ SANS AUTORISATION ÉCRITE
© ÉHO.LINK - 2024, Tous droits réservés

Filtrage réseau

La solution Ého.Link peut bloquer les utilisateurs qui tentent de se connecter à des sites malveillants via plusieurs méthodes de filtrage et elle est configurable uniquement par les administrateurs métiers :

- Filtrage DNS
  Le paramétrage du filtrage DNS se fait via l'interface Ého.My
  Les fonctionnalités sont :
  - Interception des requêtes DNS (protocole DNS uniquement)
  - Catégorisation des noms de domaine fournie par BrightCloud
  - Acceptation/refus

- Filtrage des paquets malformés
  Ce comportement n'est pas configurable.
  Les paquets malformés (IP, TCP, UDP, ICMP...) ne sont pas transmis sur le réseau.

- IDS / IPS
  Le paramétrage se fait via l'interface Ého.My.
  - Activé par défaut
  - Possibilité de désactiver le blocage des flux sur la génération d'une alerte

  Les fonctionnalités sont basées sur :
  - Une base de données de signatures mise à jour plusieurs fois par semaine (à travers Ého.Cloud)
  - Une détection de signatures sur les protocoles ICMP, ICMPv6, IP, UDP, TCP, HTTP, TLS...
  - Une remontée des alertes vers le cloud client.

  La détection d'intrusion en tant que mécanisme ne fait pas partie du périmètre d'évaluation.

- Filtrage protocolaire
  Ce comportement n'est pas configurable.
  Les fonctionnalités sont :
  - Détection automatique du protocole utilisé par un flux donné
  - Blocage du flux

  A date, seul le protocole QUIC est bloqué

Contrôle d'accès données globales bénéficiaires (Ého.My)

Les données statistiques globales sont non modifiables et accessibles uniquement aux utilisateurs authentifiés et aux administrateurs métier, chaque bénéficiaire est cloisonné dans un container LXD différent.

CE DOCUMENT EST LA PROPRIÉTÉ DE ÉHO.LINK ET NE PEUT ÊTRE REPRODUIT OU COMMUNIQUÉ SANS AUTORISATION ÉCRITE
© ÉHO.LINK - 2024, Tous droits réservés

Authentification

La solution Ého.Link est capable :

- D'identifier les utilisateurs finaux et administrateurs métier, qui doivent s'authentifier avec un mot de passe.
- De contrôler l'accès aux fonctions d'administration et de toutes informations des utilisateurs pour les administrateurs métier.
- Et pour les utilisateurs finaux de contrôler l'accès à leurs informations personnelles.

Utilisation d'un nonce permettant de rendre unique dans le temps les valeurs nécessaires à l'identification d'un utilisateur.

Les jetons de session sont protégés contre le vol et contre le rejeu. Les jetons de session ont une durée de vie limitée.

Les secrets de connexion des utilisateurs sont stockés de manière sécurisée sur la solution Ého.Link et la compromission d'un fichier ne permet pas de les récupérer, ils sont stockés sont forme de hash (SHA3-256).

Communications sécurisées

Les communications avec la solution Ého.Link sont protégées en confidentialité et en intégrité grâce au protocole TLS.

Échanges internes Ého.Box / Ého.Cloud (utilisé seulement par l'infrastructure, non accessible par le bénéficiaire)

- Ého.Box (BOX_ FACTORY)
  - Clé RSA 2048
  - Signature SHA256
  - Certificat x509

- Ého.Box (BOX_CUSTOMER)
  - Clé RSA 2048
  - Signature SHA256
  - Certificat x509

- Ého.Cloud (CONTAINER_CUSTOMER)
  - Clé RSA 4096
  - Signature SHA256
  - Certificat x509

Échanges internes Ého.My/Ého.Cloud (utilisé seulement par l'infrastructure, non accessible par le bénéficiaire)

- Ého.Cloud (CONTAINER_SERVICE)
  - Clé RSA 4096
  - Signature SHA256
  - Certificat x509

- Ého.My (SERVER)
  - Clé RSA 4096

CE DOCUMENT EST LA PROPRIÉTÉ DE ÉHO.LINK ET NE PEUT ÊTRE REPRODUIT OU COMMUNIQUÉ SANS AUTORISATION ÉCRITE
© ÉHO.LINK - 2024, Tous droits réservés

- Signature SHA256
- Certificat x509

Échanges publiques signés par GlobalSign (utilisé par le bénéficiaire)

- STATUS
  - Clé RSA 2048
  - Signature SHA256
  - Certificat x509

- PUBLIC
  - Clé RSA 2048
  - Signature SHA256
  - Certificat x509

Administration sécurisée à distance

Les administrateurs systèmes peuvent se connecter à une Ého.Box au moyen d'un service SSH et OpenVPN :

- Création d'un tunnel OpenVPN vers l'infra Ého.Link
- Connexion SSH sur un cloud client
- Création d'un tunnel SSH vers une box associée à ce cloud client, en passant dans le tunnel VPN situé entre cette box et cloud

Chaque étape nécessite un certificat protégé par un HSM

- Tunnel VPN (vers infrastructure Ého.Link) : Clé stockée sur une clé HSM Nitrokey
  - Cipher AES-256-CBC
  - auth SHA256
  - Double authentification avec TLS 1.3, certificat :
    - Clé RSA 4096
    - Signature SHA256
    - Certificat x509
- Connexion SSH vers un cloud client => clé stockée dans la Nitrokey
  - RSA 4096
- Tunnel SSH vers la box => clé stockée dans la Nitrokey
  - RSA 4096

Mise à jour de la base de signatures

L'IDS propose une fonctionnalité de mise à jour de la base de signatures. Pour ce faire, l'Ého.Box se connecte périodiquement afin de vérifier si une nouvelle base de signatures est disponible. La mise à jour est automatisée. Cette fonction de sécurité est renforcée par une fonctionnalité de contrôle automatique de la base de signatures activée lors d'une opération de mise à jour. Ce processus permet d'éviter que l'IDS dispose d'une base de signatures incomplète ou non fonctionnelle en cas d'échec de la mise à jour.
Intégrité garantie pendant le transport (tunnel chiffré) mais pas à l'utilisation.

CE DOCUMENT EST LA PROPRIÉTÉ DE ÉHO.LINK ET NE PEUT ÊTRE REPRODUIT OU COMMUNIQUÉ SANS AUTORISATION ÉCRITE
© ÉHO.LINK - 2024, Tous droits réservés

Génération de journaux d'évènements

Les journaux sont non modifiables et accessibles uniquement aux utilisateurs authentifiés autorisés. Les journaux sont générés et stockés en local sur le système de fichier persistant qui est chiffré puis transmis tant que l'Ého.Box est connectée sur Ého.Cloud. En cas de saturation, les journaux les plus anciens sont supprimés par le mécanisme définit par syslog-ng.

Protection des clés

Sur Ého.My et Ého.Cloud, les clés ne sont accessibles qu'aux administrateurs de l'infrastructure technique et système grâce aux mécanismes de gestion des droits de linux.
Sur l'Ého.Box les clés du Secureboot sont stockées dans le processeur et accessibles uniquement durant le boot. La clé KAK est fusée à la fabrication de l'Ého.Box.
Pour la clé STATUS elle est stockée dans le firmware et elle n'est accessible qu'aux administrateurs de l'infrastructure technique et système grâce aux mécanismes de gestion des droits de linux.
Pour les autres clés, elles sont stockées dans le TPM et seules les clés publiques sont accessibles. Pour la clé LUKS TPM, elle est en plus protégée par le mécanisme de mesure du TPM qui ne permet son accès que si le TPM reçoit les bonnes valeurs. Ces valeurs sont définies uniquement durant l'étape du déchiffrement du rootfs lors du boot.

CE DOCUMENT EST LA PROPRIÉTÉ DE ÉHO.LINK ET NE PEUT ÊTRE REPRODUIT OU COMMUNIQUÉ SANS AUTORISATION ÉCRITE
© ÉHO.LINK - 2024, Tous droits réservés

Menaces et biens sensibles

Menaces	Biens sensibles
Corruption du firmware	Firmware d'Ého.Box
Contournement de la politique de filtrage	Politiques de filtrage réseau
Accès illicite hors bénéficiaire	Base d'identification utilisateurs
Accès illicite intra bénéficiaire	Base d'identification utilisateurs
Accès illicite extra bénéficiaire	Base d'identification utilisateurs
Élévation de privilège	Données statistiques des bénéficiaires Politique d'accès réseaux
Corruption des mises à jour IDS	La base de signatures
Accès aux journaux	Les journaux d'audit et d'alertes
Corruption des flux	Flux Bénéficiaires internet Flux Bénéficiaires de configuration Flux Ého.Box/Ého.Cloud Flux Ého.My/Ého.Cloud
Vol de clés	Clés Ého.Box Clés Ého.Cloud Clés Ého.My Clés pour l'administration SSH à distance des Ého.Box
Accès illicite Ého.Box	Firmware d'Ého.Box

CE DOCUMENT EST LA PROPRIÉTÉ DE ÉHO.LINK ET NE PEUT ÊTRE REPRODUIT OU COMMUNIQUÉ SANS AUTORISATION ÉCRITE
© ÉHO.LINK - 2024, Tous droits réservés

Menaces et fonctions de sécurité

Menaces	Fonctions de sécurité permettant de contrer les menaces
Corruption du firmware	Bootloader sécurisé Mise à jour du firmware
Contournement de la politique de filtrage	Filtrage réseau
Accès illicite hors bénéficiaire	Authentification
Accès illicite intra bénéficiaire	Authentification
Accès illicite extra bénéficiaire	Authentification
Élévation de privilège	Contrôle d'accès données globales bénéficiaires (Ého.My)
Corruption des mises à jour IDS	Mise à jour de la base de signatures
Accès aux journaux	Authentification Génération de journaux d'évènements
Corruption des flux	Communications sécurisées
Vol de clés	Protection des clés
Accès illicite Ého.Box	Administration sécurisée à distance

Documents de référence

- ANSSI-CSPN-CER-P-01 version 5.0
- ANSSI-CSPN-NOTE-06 version 1.0

CE DOCUMENT EST LA PROPRIÉTÉ DE ÉHO.LINK ET NE PEUT ÊTRE REPRODUIT OU COMMUNIQUÉ SANS AUTORISATION ÉCRITE
© ÉHO.LINK - 2024, Tous droits réservés