BREVET DE TECHNICIEN SUPÉRIEUR
SERVICES INFORMATIQUES AUX ORGANISATIONS
Option : Solutions d'infrastructure, systèmes et réseaux

U7 – CYBERSÉCURITÉ DES SERVICES INFORMATIQUES

SESSION 2025

_____

Durée : 4 heures
Coefficient : 4

_____

Matériel autorisé :
Aucun matériel ni document n'est autorisé.

Dès que le sujet vous est remis, assurez-vous qu'il est complet.

Le sujet comporte 18 pages, numérotées de 1/18 à 18/18.

Cas Everest

Ce sujet comporte 18 pages dont un dossier documentaire de 10 pages.

Barème

DOSSIER A	**Intégration de la structure KliK**	30 points
DOSSIER B	**Gestion des journaux**	50 points
	TOTAL	80 points

Dossier documentaire

Présentation du contexte

Everest est le numéro un français des progiciels de gestion d'affaires. Cette entreprise bénéficie actuellement de la confiance de 3 700 sociétés de services et propose une gamme de solutions comprenant un logiciel de gestion de la relation client (Clientor), des logiciels de gestion d'affaires (Projector-G et Projector-X) et un portail *web* Visior. Les clients d'Everest sont à la fois des TPE[1], PME[2] et GME[3], dans des secteurs d'activités variés.

Everest compte actuellement 227 collaborateurs répartis sur 10 sites (siège et agences) en France, dont certains réalisent de la prospection en télétravail. Le siège social de l'entreprise est à Lyon, tout comme le service support et développement du produit Projector-X.

Face à une concurrence rude, notamment avec l'arrivée des solutions gratuites, Everest doit changer son modèle commercial et faire évoluer ses offres de produits et services.

Les produits d'Everest sont proposés sous différentes formes afin de s'adapter aux besoins et aux budgets des clients :

- **Logiciels sur site** : les logiciels Everest sont installés sur les serveurs des clients. Cette installation peut être réalisée sur place ou à distance.
- **SaaS** (*software as a service* ou logiciel à la demande) : Everest utilise des serveurs dans un centre de données (*datacenter*) externe à l'entreprise et met à disposition des clients une instance de leur produit.

Régulièrement, les clients principaux font réaliser des audits de sécurité de leurs outils par des entreprises spécialisées en cybersécurité. Des rapports sont alors transmis à Everest pour leur demander d'améliorer la sécurité de leurs logiciels.

Everest vient très récemment de faire l'acquisition d'une nouvelle structure KliK, située à Paris, spécialisée dans l'informatique décisionnelle[4]. Cette entité n'est pas encore intégrée au système d'information d'Everest.

Le service informatique de l'entreprise Everest est dirigé par M. Rizzo et est composé de 5 personnes qui ont la charge de la maintenance des serveurs internes, des serveurs du centre de données et de l'intégration des nouvelles structures.

Vous travaillez au sein de cette équipe, vous avez pour mission de mener à bien les tâches suivantes :

- Intégration de la nouvelle structure KliK dans le système d'information d'Everest.
- Gestion des journaux de l'entreprise.

Vous vous appuierez sur le dossier documentaire mis à votre disposition.

[1] TPE : très petites entreprises

[2] PME : petites et moyennes entreprises

[3] GME : grandes et moyennes entreprises

[4] L'informatique décisionnelle désigne l'ensemble des méthodes et outils informatiques utilisés généralement pour piloter une organisation.

Dossier A – Intégration de la structure KliK

Pour faciliter l'intégration de la nouvelle structure KliK située à Paris, M. Rizzo a décidé d'auditer son infrastructure actuelle afin d'organiser sa connexion au siège de Lyon. Vous participez à ces travaux.

Mission A1 – Auditer le système d'authentification

Votre responsable vous charge de l'audit du système d'authentification, basé sur un domaine *Active Directory* spécifique à cette entité.

En réalisant des recherches sur internet afin de réaliser votre mission, vous découvrez l'outil d'analyse *PingCastle* qui fournit un score indiquant le niveau de risque du domaine *Active Directory*. L'outil *PingCastle* génère un rapport donnant les points à modifier pour renforcer la sécurité du système.

Le résultat de ce rapport est fourni dans le dossier documentaire.

Vous devez faire un état des lieux des menaces et intervenir sur les points critiques.

Question A1.1
Relever trois risques majeurs, en relation avec l'authentification, présents dans le rapport généré par l'outil *PingCastle*. *Justifier la réponse.*

Par ailleurs, l'indication « LAPS ne semble pas installé » a attiré votre attention. Vous étudiez une documentation sur ce sujet.

Après examen de tous les ordinateurs de l'organisation KliK, vous constatez qu'ils disposent du même compte « Administrateur local » et du même mot de passe.

Question A1.2
Rédiger la partie du rapport d'audit sur ce point, en expliquant au moins un problème de sécurité lié à l'utilisation d'un mot de passe d'administrateur local identique sur toutes les machines.

La mise en place de la solution *Microsoft LAPS* intéresse M. Rizzo qui décide de profiter de l'intégration de KliK pour réaliser une première installation. Il vous charge d'écrire la procédure d'installation adaptée à l'organisation.

Question A1.3
Définir la valeur des différents paramètres à configurer dans la stratégie de groupe (GPO) LAPS. *Justifier la réponse.*

Mission A2 – Mettre en place l'interconnexion entre les entités Everest et KliK

Le réseau de connexion inter-sites actuel d'Everest est basé sur une technologie MPLS dans laquelle les sites sont tous reliés par des liens dédiés gérés par l'opérateur SFR.

Pour cette nouvelle entité de Paris, M. Rizzo a décidé, pour des raisons économiques, d'utiliser une technique de réseau privé virtuel (VPN) IPSEC sur internet. Il vous demande de faire des choix technologiques.

Les utilisateurs de KliK ont, bien entendu, besoin d'accéder à des services d'internet. Une fois la connexion VPN mise en place, 2 solutions sont envisageables :

1. Utilisation directe de la connexion internet de KliK pour naviguer sur internet.
2. Utilisation de la liaison VPN jusqu'à Lyon et utilisation de la connexion internet de Lyon pour naviguer sur internet.

M. Rizzo s'interroge sur l'opportunité de choisir l'une ou l'autre solution.

Question A2.1
Citer au moins un argument en faveur de chacune des deux solutions pour l'aider dans son choix.

Quelle que soit la solution retenue, M. Rizzo souhaite contrôler et limiter l'utilisation d'internet des utilisateurs et mettre en place un suivi détaillé de l'activité en ligne de chacun.

Question A2.2
a) Proposer une solution pour contrôler et limiter l'utilisation d'internet par les salariés de l'entreprise.
b) Citer et expliquer la recommandation de la CNIL aux employeurs concernant le filtrage et le contrôle de la connexion internet.

Mission A3 – Centraliser l'administration réseau

Dans certains sites, dont celui de Lyon, le routeur/pare-feu permettant l'accès à internet est un modèle Meraki de Cisco.

M. Rizzo souhaite étendre cette solution progressivement à tous les sites et en faire rapidement bénéficier le site de Paris (de l'entité KliK). Avant d'investir une somme importante, il veut vérifier que cette solution est adaptée à l'entreprise Everest.

Question A3.1
Préparer une note qui détaille deux inconvénients en matière de sécurité de la solution Meraki comparée à du matériel administré localement.

M. Rizzo a effectué des recherches de son côté et a trouvé une alerte CVE (*common vulnerabilities and exposures* ou vulnérabilités et expositions communes) concernant la solution Cisco Meraki.

Il a besoin d'explications complémentaires.

Question A3.2
Lister les conséquences d'une exploitation de la vulnérabilité décrite dans l'alerte pour l'entreprise Everest.

Dossier B – Gestion des journaux

Actuellement, les journaux des matériels actifs (routeurs, commutateurs, etc.) et des serveurs (NAS, etc.) des agences ne sont pas gérés par le siège.

Afin de se prémunir en cas d'attaques, le service informatique souhaite mettre en place une solution de gestion de journaux des serveurs et des matériels actifs qui permette de garder la trace des événements en respectant les recommandations de l'ANSSI.

Vous êtes chargé(e) de la préparation de ce dossier et vous devez mettre en œuvre la gestion des journaux de l'agence de Bordeaux vers le siège de Lyon.

Mission B1 – Gérer les risques

Vous commencez votre étude par le recensement des vulnérabilités et des risques d'une solution de gestion centralisée des journaux utilisant le protocole Syslog.

Tout d'abord, vous vous rendez compte que les serveurs Syslog sont sujets aux attaques par rejeu[5]. La probabilité d'une telle attaque est assez faible si les recommandations de l'ANSSI sont appliquées, mais la gravité atteindrait un niveau important.

Question B1.1

a) Donner le niveau de criticité selon l'AFNOR de ce type d'attaque si elle se produisait sur le serveur de journaux en justifiant votre réponse.
b) Préciser le niveau de risque selon l'AFNOR qui découle de ce type d'attaque.

Vous vous penchez sur les faiblesses du protocole Syslog lors du transfert des informations dans son fonctionnement natif. Vous décidez d'évaluer les conséquences sur la sécurité.

Votre étude vous a permis de déceler deux attaques courantes sur le protocole Syslog.

Question B1.2

Lister les conséquences en matière d'intégrité et de disponibilité pour chacune des deux attaques.

Ces faiblesses étant inhérentes au mode natif, votre responsable envisage d'utiliser le mode sécurisé du protocole : Syslog sur TLS (*Syslog over TLS*). Aussi, il vous demande de lui rédiger une note à ce sujet.

Question B1.3

Expliquer en quoi l'utilisation de certificats permet d'assurer les fonctions d'authentification, de confidentialité et d'intégrité pour la transmission des informations.

Vous poursuivez votre étude sur la gestion des journaux et votre responsable vous demande de la prudence concernant le volume d'informations transmises par le protocole.

Question B1.4

Expliquer au moins une conséquence en matière de sécurité :

a) si tous les journaux (quel que soit leur volume et leur type) sont transmis au serveur central,

b) si seules les informations d'erreurs sont transmises.

[5] Une attaque par rejeu est une forme d'attaque réseau dans laquelle une transmission est malicieusement répétée par un attaquant qui a intercepté la transmission. Il s'agit d'un type d'usurpation d'identité.

À la suite de cette analyse, vous cherchez à évaluer quelles sont les informations pertinentes à rassembler. Vous devez définir pour chaque cas, une priorité à configurer dans chaque équipement.

Question B1.5
a) Calculer la priorité d'un message Syslog en cas d'erreur de fonctionnement dans le noyau et donner la syntaxe de son sélecteur.
b) Calculer la priorité d'un message Syslog à intégrer sur un équipement en cas d'élévation de privilèges et donner la syntaxe de son sélecteur.

Mission B2 – Étudier le positionnement d'un serveur de journaux

L'entreprise possède des agences distantes et l'envoi de journaux vers le siège doit être protégé de coupures internet ou d'autres défaillances.

Question B2.1
Donner l'emplacement des relais, collecteurs et périphériques à installer à Bordeaux et à Lyon pour mettre en place une infrastructure d'envoi de journaux résiliente.

Cependant, à la lecture des bonnes pratiques de l'ANSSI, vous alertez votre responsable sur le manque de protection du serveur de collecte.

Question B2.2
Proposer une solution de segmentation qui permette de cloisonner le serveur de collecte.

Votre responsable a choisi de positionner des relais dans chaque agence et vous demande de prévoir l'organisation du stockage de messages sur le collecteur central.

Les journaux peuvent être stockés dans des dossiers différents en fonction de leur provenance, de leur horodatage, de leur priorité ou de leur type. Vous vous interrogez sur l'arborescence de répertoire à mettre en place mais votre responsable choisit de mettre en place une arborescence par agence.

Question B2.3
Choisir la fonction de filtrage à utiliser afin de stocker les journaux dans un dossier par agence. *Justifier la réponse.*

Afin de mettre en œuvre votre solution, votre responsable hésite entre installer le service de centralisation des journaux sur le serveur de supervision "KRYPTON" ou dédier un serveur spécifique à cette fonction. Il vous demande de l'aider dans son choix.

Question B2.4
a) Expliquer les interactions entre le serveur de supervision et le serveur de journalisation.
b) Citer deux arguments en faveur d'une solution de gestion des journaux séparée de celle de la supervision.

Votre responsable a validé votre dossier technique. Un nouveau serveur "NEPTUNE" a été installé pour accueillir le serveur de collecte.
Vous préparez maintenant la mise en œuvre de la gestion des journaux sur le site de Bordeaux.

Question B2.5
Écrire les commandes qui permettent d'activer le protocole Syslog du pare-feu Cisco de Bordeaux afin d'envoyer tous les messages d'authentification dont la gravité est strictement inférieure à 5.

Mission B3 : Gérer les sauvegardes

Pour que votre solution soit complète, vous préparez la sauvegarde du serveur de journaux.

Alerté par l'augmentation des attaques par rançongiciel (*ransomware*) qui peuvent se produire dans ce cadre, vous proposez de mettre en place la politique de sauvegarde la plus sûre.

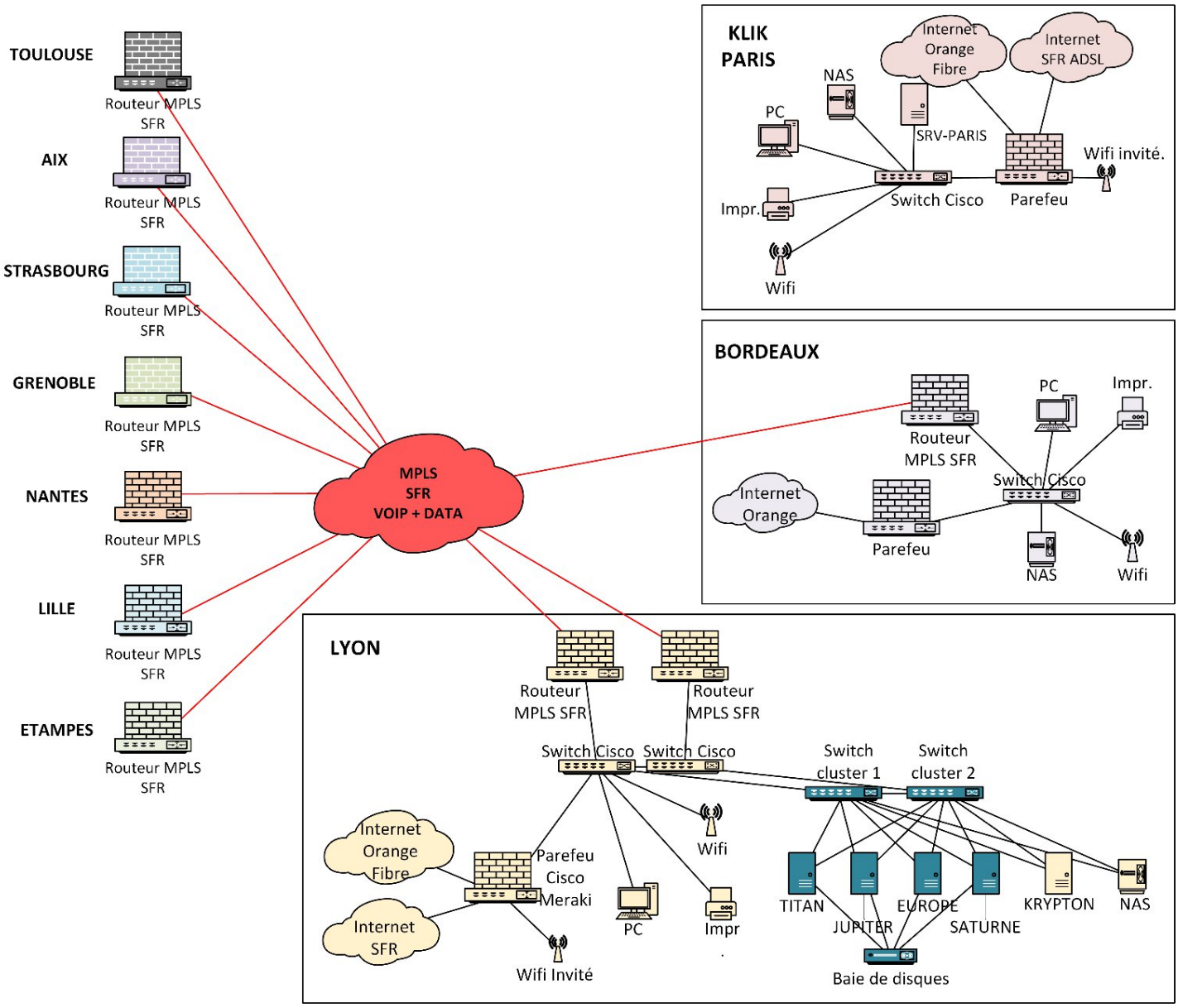
Question B3.1
Expliquer en quoi les deux 1 et le 0 de la politique « 3-2-1-1-0 » limitent les risques de corruption des supports de sauvegarde.

Une partie des journaux trace l'activité des utilisateurs et est de ce fait sauvegardée. On y retrouve l'identifiant de chaque internaute, la date et l'heure de sa connexion et le détail des opérations effectuées.

Question B3.2
Rappeler les précautions à prendre, d'après les recommandations de la CNIL et du RGPD, dans le cadre de la collecte et de la sauvegarde de ces journaux.

Documents communs aux dossiers A et B

Document 1 : Schéma réseau de l'infrastructure actuelle



Toutes les agences disposent d'une infrastructure système et réseau identique à celle de l'agence de Bordeaux.

Document 2 : Rôles des serveurs

EUROPE SATURNE	Serveurs de développement en grappe (*cluster*)
TITAN JUPITER	Serveurs redondants d'infrastructure : Active Directory, DNS, DHCP
KRYPTON	Serveur de supervision

Documents associés au dossier A

Document A1 : Rapport PingCastle

Un rapport PingCastle indique un score de niveau de risque. Plus le score est élevé, plus le risque est important. Ainsi, un score de 0 représente un domaine parfaitement sécurisé.

KliK.local

Version moteur : 2.4.3.0

Indicateurs Active Directory

Indicateurs

Niveau de risque du domaine : 76 / 100

Il s'agit du score maximum des 4 indicateurs et un score ne peut être supérieur à 100.

Objet périmé : 76 /100	Il s'agit d'opérations liées aux objets utilisateur ou informatiques	7 règles correspondent	Fiducies : 0 /100	Il s'agit de liens entre deux Active Directory	0 règle correspondante
Comptes privilégiés : 35 /100	Il s'agit des administrateurs de l'Active Directory	3 règles correspondent	Anomalies : 65 /100	Il s'agit de points de contrôle de sécurité spécifiques	5 règles correspondent

Présence de Windows 2003 = 1	*+ 20 points*
Présence de Windows XP = 8	*+ 15 points*
Comptes pouvant avoir un mot de passe vide (peut être remplacé par GPO) = 1 (>0)	*+ 15 points*
Comptes d'ordinateurs inactifs = 59 (26 % représentent plus de 15 % de tous les ordinateurs)	*+ 10 points*
LAPS ne semble pas être installé	*+ 10 points*
Les utilisateurs non administrateurs peuvent ajouter jusqu'à 10 ordinateurs à un domaine	*+ 10 points*
SMB v1 activé sur 2 DC	*+ 1 point*
La dernière sauvegarde AD date du 26/10/2021 à 02:28:24Z, il y a plus de 24 heures.	*+ 15 points*
Dernière modification du mot de passe Kerberos : 13/01/2020 16:16:09	*+ 50 points*
Présence de comptes de service dans le groupe admin du domaine (au moins 2 comptes ont un mot de passe qui n'expire jamais) : 14	*+ 15 points*

Document A2 : Description de la solution Microsoft LAPS

Qu'est-ce que Microsoft LAPS ?

La « solution de mot de passe d'administrateur local » (LAPS, *local administrator password solution*) de Microsoft fournit des capacités de gestion des mots de passe des comptes d'administrateur local pour les ordinateurs joints à un domaine. Les mots de passe sont aléatoires et stockés dans l'annuaire *Active Directory* (AD), protégés par des listes de contrôle d'accès. Par conséquent, seuls les utilisateurs éligibles peuvent les lire ou demander leur réinitialisation.

Quel risque prend une organisation si elle n'implémente pas la solution LAPS ?

LAPS fournit une solution au problème lié à l'utilisation d'un compte local commun avec un mot de passe identique sur chaque ordinateur d'un domaine. Elle résout ce problème en définissant un autre mot de passe aléatoire différent pour le compte d'administrateur local commun sur chaque ordinateur du domaine.

LAPS simplifie la gestion des mots de passe tout en permettant aux clients d'implémenter des défenses recommandées supplémentaires contre les cyberattaques. En particulier, la solution réduit le risque d'escalade latérale qui en résulte quand des clients utilisent la même combinaison et le même mot de passe de compte local administratif sur leurs ordinateurs. Elle stocke le mot de passe du compte d'administrateur local de chaque ordinateur dans l'annuaire AD et le sécurise dans un attribut confidentiel de l'objet correspondant de l'ordinateur. L'ordinateur peut mettre à jour ses propres données de mot de passe dans l'annuaire AD et les administrateurs de domaine peuvent accorder un accès en lecture à des utilisateurs ou groupes autorisés, comme les administrateurs de support technique des stations de travail.

Source : https://learn.microsoft.com/fr-fr/defender-for-identity/security-assessment-laps

Document A3 : Mise en place de la solution Microsoft LAPS

Principales étapes :

- Installation de Microsoft LAPS sur le contrôleur de domaine.
- Préparation du schéma *Active Directory* pour LAPS.
- Préparation de la stratégie de groupe LAPS.
- Déploiement du client LAPS sur les machines à gérer.

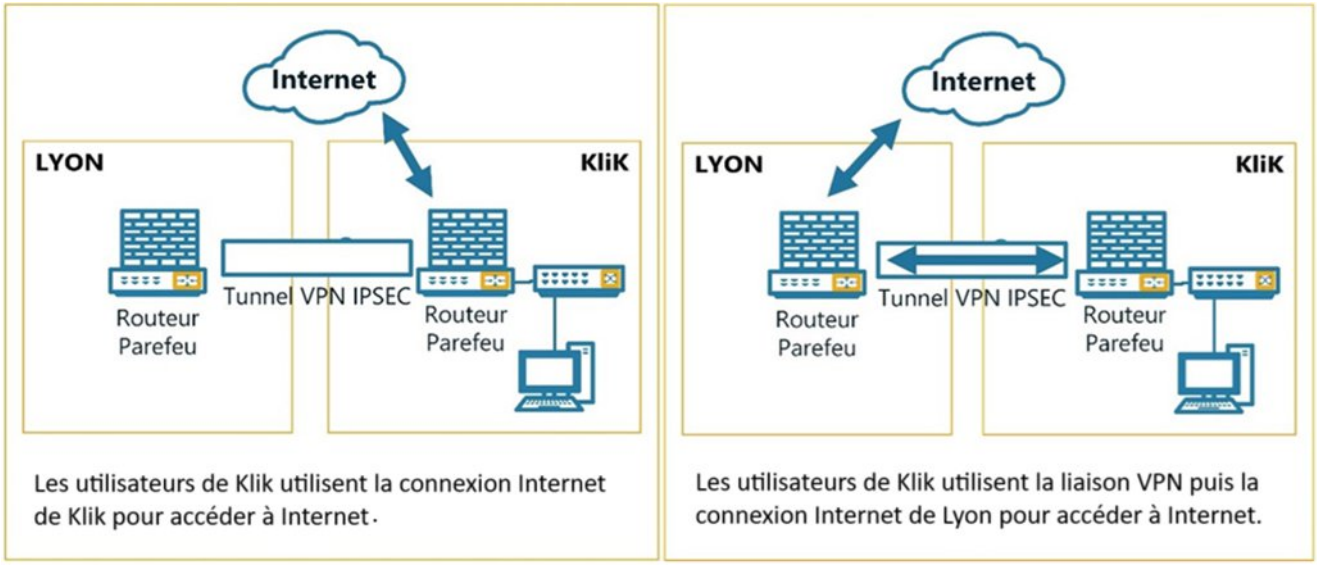
Stratégie de groupe LAPS, principaux paramètres :

Paramètre	Valeurs
Configuration mot de passe	
Complexité mot de passe	Majuscules Majuscules+minuscules Majuscules+minuscules+nombres Majuscules+minuscules+nombres+caractères spéciaux.
Longueur mot de passe	8 – 64 caractères
Durée de vie mot de passe	1 – 365 jours
Nom du compte administrateur à gérer (*)	(Par défaut = Administrateur)
Ne pas autoriser une expiration du mot de passe plus longue que le permet la stratégie définie au sein du paramètre "Configuration mot de passe".	Activé Désactivé
Activer ou désactiver la gestion du mot de passe administrateur avec LAPS pour l'ordinateur cible	Activé Désactivé

(*) Permet de définir un compte administrateur à configurer autre que le compte nommé « Administrateur » intégré à Windows.

Source : Les auteurs

Document A4 : Solutions de connexion internet des utilisateurs de l'entité KliK



Source : Les auteurs

Document A5 : Présentation de la solution VPN IPSEC

Le protocole IPSec (*IP Security Protocol*) est développé par l'organisme IETF (*Internet Engineering Task Force*), dont le but est de sécuriser la connexion TCP/IP par l'authentification et le chiffrement des paquets IP. Le protocole IPSec est de niveau 3 du modèle OSI. Configuré en mode tunnel, il permet le chiffrement de la charge utile IP, l'encapsulation dans un autre paquet IP, et l'envoi à travers un réseau intermédiaire IP comme Internet.

Le protocole IPSec assure donc en théorie une bonne interopérabilité entre les différents matériels. Se situant au niveau de la couche réseau, les applications n'ont pas à se soucier de l'implémentation du protocole IPSec.

Source : Guillaume HUGUES

Document A6 : Présentation de la solution Cisco Meraki

Gérez votre réseau entièrement grâce au nuage (cloud).

Meraki est une solution réseau entièrement gérée dans le nuage (*cloud*), intuitive et sécurisée, pour répondre à tous vos besoins.

Elle dispose d'une plate-forme unique, personnalisable, qui vous permet de gérer à distance tous vos périphériques depuis un simple navigateur et en toute sécurité.

La grande révolution des solutions Cisco Meraki est l'offre Cloud Controller.

Cette plateforme permet la configuration des équipements pré et post déploiement. Cela permet de réduire considérablement le temps consacré à leur installation et utilisation.

Les avantages de cette technologie sont nombreux :

- Simplification de l'architecture réseau traditionnelle grâce aux « contrôleurs » hébergés directement chez Cisco. Plus besoin de maintenance.
- Installation facilitée grâce aux bornes *plug&play* avec leur configuration automatique depuis la plate-forme *Cloud Controller*.
- Gestion centralisée accessible depuis un simple navigateur internet.
- Mises à jour gérées directement par le constructeur.
- Authentification par utilisateur/mot de passe ou multifacteur.

Source : *compufirst.com*

Document A7 : Avis du Cert-Fr – Vulnérabilités dans les produits Cisco

Date de publication : 21/10/2022

CVE-2022-20933 [Score CVSS[6] v3.1: 8.6]

Un défaut de vérification des données envoyées lors de l'initialisation d'une connexion VPN AnyConnect vers un routeur Meraki MX ou Z3 permet à un attaquant non authentifié, en envoyant une requête spécifiquement forgée, de provoquer un déni de service de l'équipement.

Risque	Déni de service
Criticité	Score CVSS v3.1: 8.6 max
La faille est activement exploitée	Non
Un correctif existe	Oui
Une mesure de contournement existe	Oui
La vulnérabilité exploitée est du type	CWE-234 : Échec à gérer le paramètre manquant
Détails sur l'exploitation	Vecteur d'attaque : réseau. Complexité de l'attaque : faible. Privilèges nécessaires pour réaliser l'attaque : non. Interaction d'un utilisateur ayant accès au produit est-elle nécessaire : non. L'exploitation de la faille permet d'obtenir des droits privilégiés : non.
Solutions ou recommandations	Mettre à jour les routeurs Cisco Meraki vers les versions 16.16.6, 17.10.1 ou vers une version supérieure. Il est possible de se protéger de la vulnérabilité en désactivant le VPN Cisco AnyConnect.

[6] Common Vulnerability Scoring System (CVSS) est un système d'évaluation standardisé de la criticité des vulnérabilités selon des critères objectifs et mesurables. Le score final est compris entre 0 et 10, 10 correspondant aux vulnérabilités les plus critiques.

Documents associés au dossier B

Document B1 : Présentation du protocole Syslog

Le protocole Syslog (*System Logging Protocol*) est défini dans le document RFC 5424 et désigne un protocole standard qui sert à envoyer des fichiers du journal système ou des messages ayant trait à des événements à un serveur dédié appelé « serveur syslog ». On l'utilise avant toute chose pour collecter différents journaux d'événements auprès de plusieurs machines et pour les transférer vers un emplacement central depuis lequel on pourra les consulter et les examiner.
Le protocole est activé sur la plupart des périphériques réseaux tels que les routeurs, les commutateurs, les pares-feux, et même certains modèles d'imprimantes. Il est aussi disponible sur les systèmes de type Unix et Linux et sur quantité de serveurs *web* dont Apache.

Une des grandes limites du protocole Syslog est que l'appareil sous surveillance ne peut générer ou envoyer un événement Syslog qu'à la condition d'être opérationnel et connecté au réseau.

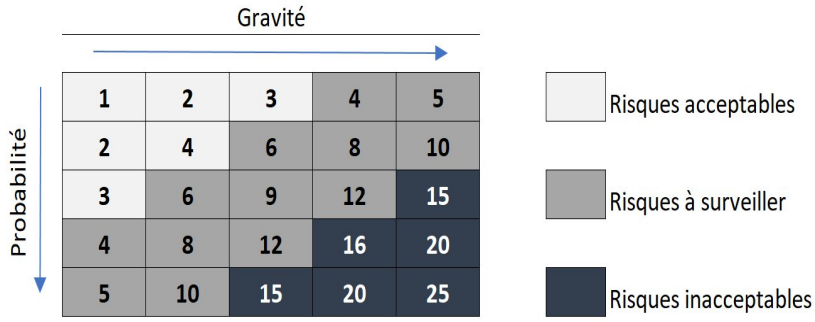
Source : https://www.paessler.com/fr/it-explained/syslog

Document B2 : Gestion des risques selon l'AFNOR

Définition de la probabilité	
Note	Probabilité
1	Minimale
2	**Faible**
3	**Elevée**
4	**Forte**
5	**Maximale**

Définition de la gravité	
Note	Gravité
1	Négligeable
2	**Notable**
3	**Important**
4	**Critique**
5	**Catastrophique**

Attribuer un score de probabilité et de gravité à chaque risque, sert à calculer la criticité. Selon l'AFNOR, la **criticité** d'un risque résulte de la multiplication de la gravité par la probabilité d'un risque.
Une matrice des risques peut donc être réalisée afin de classer les risques au rang d'acceptable ou non.



Document B3 : La sécurité du protocole Syslog

Le protocole Syslog, par défaut, fonctionne en UDP avec le port 514. Les informations circulent en clair sur le réseau. Syslog peut être également configuré en mode TCP.

Syslog est susceptible de subir différentes attaques.

Attaque 1 :
Il est possible de fabriquer de toutes pièces une trame Syslog et de l'envoyer à un serveur Syslog en falsifiant l'adresse IP et/ou l'adresse Mac de l'émetteur de la trame.

Attaque 2 :
Il est possible de « bombarder » un serveur Syslog avec des trames Syslog de manière à occuper le serveur Syslog et noyer des événements réels parmi un grand nombre de messages falsifiés. Ces messages falsifiés peuvent avoir pour but de remplir le disque dur du serveur Syslog.

Source : https://ram-0000.developpez.com/tutoriels/reseau/Syslog/

Document B4 : Composition d'un message Syslog

La plupart des implémentations Syslog permettent de paramétrer les fonctionnalités et les seuils de gravité qui génèreront des événements Syslog destinés à être transférés au serveur Syslog.

Un message Syslog se compose de 3 parties :

- le niveau de priorité calculé (PRI),
- l'en-tête comportant les informations d'identification (HEADER),
- le message lui-même (MSG).

Les données PRI envoyées via le protocole Syslog sont le fruit de deux valeurs qui permettent de classifier le message.

La première valeur est la catégorie identifiée par une valeur « Facility value ». Elle correspond à une des 15 valeurs prédéfinies. Elles assignent une catégorie au type de message ou au système à l'origine de l'événement.

Facility value	Catégorie ou système à l'origine de l'événement
0	kern : messages provenant du noyau (cœur du système d'exploitation)
1	user : messages utilisateur (générique)
2	mail : provient de la messagerie électronique
3	daemon : messages des processus d'arrière-plan
4	auth : messages d'authentification
5	syslog : message du serveur syslogd lui-même
6	ipr : provient du sous-système d'impression
7	news : messages d'actualités
8	uucp : messages du sous-système UUCP (obsolète)
9	authpriv : sécurité, élévation de privilèges
10	ftp : concerne le serveur FTP
11	synchronisation NTP
12	log audit
13	log alert
14	cron : provient des services de planification de tâches

La seconde valeur catégorise l'importance ou la gravité du message par un chiffre allant de 0 à 7.

Code	Severity	Description
0	Emergency	Système inutilisable.
1	Alert	Une intervention immédiate est nécessaire.
2	Critical	Erreur critique pour le système.
3	Error	Erreur de fonctionnement.
4	Warning	Avertissement (une erreur peut intervenir si aucune action n'est prise).
5	Notice	Événement normal méritant d'être signalé.
6	Informational	Pour information.
7	Debug	Message de mise au point.

Au sein d'un même service ou application, moins le chiffre correspondant au code est élevé, plus le problème affectant le processus en question est grave.

Les deux valeurs sont agrégées pour produire un indice de « Priorité » qui est envoyé conjointement au message. Cet indice se calcule en multipliant la catégorie par 8 et en y ajoutant le niveau de gravité. Plus le PRI est bas, plus la priorité est élevée.

Priorité = (catégorie x 8) + gravité

Configuration et syntaxe du service Syslog sur les équipements

Un sélecteur est la liste des informations que l'on souhaite que l'équipement transmette. Il est composé de « couples » de valeurs séparées par un point.

Un couple est composé d'un sous-système associé à une priorité (*severity*).

La priorité indiquée recouvre les messages de priorité supérieure ou égale.

L'astérisque représente tous les sous-systèmes ou toutes les priorités.

On peut regrouper plusieurs sous-systèmes en les séparant par une virgule (exemple : auth,mail.debug).

– Exemples :

- mail.notice messages concernant le courriel, pour tous les niveaux de « notice » à « emergency ».
- *.alert messages concernant tous les systèmes pour les niveaux «alert » à « emergency ».
- mail.* messages concernant le courrier pour tous les niveaux d'alertes.

Source : https://www.paessler.com/fr/it-explained/syslog

Document B5 : Infrastructure Syslog, notions de périphérique, de relais et de collecteur

Le protocole Syslog définit la notion de périphérique, de relais et de collecteur dans une architecture Syslog.

Un périphérique est une machine ou une application qui génère des messages Syslog.

Un relais est une machine ou une application qui reçoit des messages Syslog, les enregistre et les retransmet à une autre machine.

Un collecteur est une machine ou une application qui reçoit des messages Syslog, les enregistre mais qui ne les retransmet pas.

Tout périphérique ou relais sera vu comme un émetteur lorsqu'il envoie un message Syslog et tout relais ou collecteur sera vu comme un récepteur lorsqu'il reçoit un message Syslog.

Source : *https://ram-0000.developpez.com/tutoriels/reseau/Syslog/*

Document B6 : Recommandations de l'ANSSI (extrait 1)

Fiabilisation du transfert des journaux

Les applications de transfert de journaux reposent sur les protocoles TCP ou UDP pour acheminer les données vers les équipements centraux. Le plus simple des deux, le protocole UDP, présente l'avantage de prendre le minimum de ressources mais il a l'inconvénient d'être peu fiable car sujet aux pertes définitives de paquets. Le protocole TCP, quant à lui, améliore la fiabilité du transfert des journaux en ajoutant des fonctions de ré-émission de paquets, de mise en cache du côté de l'émetteur et d'acquittement envoyés par le destinataire.

Sécurisation du transfert des journaux

Il est nécessaire de mettre en place des mécanismes de protection garantissant la confidentialité et l'intégrité des flux de transfert des journaux, en particulier lorsque les données transitent sur des réseaux non maîtrisés. Le besoin en confidentialité est aussi fonction de la sensibilité des informations journalisées. L'idéal est de mettre en place un canal de transmission dédié réalisé à l'aide de mécanismes cryptographiques robustes.

Sécurisation des serveurs de collecte
Les informations stockées sur les serveurs de collecte sont susceptibles d'être des cibles de choix pour un attaquant cherchant à effacer ses traces, dissimuler ses activités et complexifier les activités de détection des incidents de sécurité. Il est donc indispensable de sécuriser les serveurs de collecte : la configuration système de ces serveurs doit être durcie et ils doivent être cloisonnés d'un point de vue réseau.

R12 Contrôler régulièrement la couverture de la chaîne de collecte des évènements
Il est recommandé de vérifier régulièrement que toutes les solutions logicielles des systèmes d'information (SI) sont bien journalisés et transfèrent leurs évènements à des serveurs de collecte des journaux. Le bon fonctionnement de ces serveurs de collecte (intermédiaires et centraux) doit également être vérifié en continu (supervision opérationnelle et supervision de sécurité).

R19 Durcir et maintenir à jour les serveurs de collecte
L'utilisation d'un SI d'administration dédié est une bonne pratique qui doit être privilégiée.

Lorsqu'il existe, ce SI doit être utilisé en priorité pour faire transiter les flux de collecte des journaux générés par les équipements administrés. Cette solution met à disposition de fait une bande passante plus importante sans affecter la disponibilité des services métier et peut, lorsque la sensibilité des informations transmises le justifie, apporter une protection supplémentaire.

Les serveurs de collecte, intermédiaires ou centraux, doivent être hébergés préférentiellement dans une zone dédiée du SI d'administration et sans lien logique avec les serveurs outils d'administration.

R20 Cloisonner les serveurs de collecte au sein d'un SI d'administration
Lorsque le besoin de sécurité pour le traitement des journaux est important, celui-ci doit se faire dans une zone dédiée du SI d'administration ; les serveurs de collecte intermédiaires et centraux doivent être hébergés sur ce SI d'administration.

S'il n'existe pas de SI d'administration dans l'architecture pour accueillir les serveurs de collecte intermédiaires et centraux, ils doivent être placés dans une zone interne dédiée, non exposée directement à des réseaux qui ne sont pas de confiance (par exemple Internet).

Document B7 : Recommandations de l'ANSSI (extrait 2)

Collecte et centralisation des journaux
[…] Dans certains cas, il peut être pertinent d'adopter une organisation hiérarchique du système de journalisation. Des serveurs intermédiaires collectent les journaux des équipements correspondant à leur périmètre physique ou fonctionnel, puis ils les transmettent aux serveurs de collecte centraux qui ont la charge d'agréger la totalité des journaux du SI ou d'un sous-ensemble spécifique (base de données, système, etc.). Les serveurs de collecte intermédiaires dupliquent également les journaux et les conservent localement afin d'éviter les pertes en cas de dysfonctionnement lors du transfert au niveau supérieur.

Une organisation de ce type comporte plusieurs avantages :

- la résilience de l'architecture de journalisation est meilleure : les serveurs intermédiaires peuvent pallier une indisponibilité des serveurs centraux. La copie des journaux conservée sur ces serveurs intermédiaires pourra être transmise au niveau central une fois la communication rétablie. Cela nécessite la configuration d'une politique de rétention adéquate, c'est-à-dire adaptée à la volumétrie et aux exigences de disponibilité des serveurs centraux ;
- le nombre de flux réseau de journalisation est réduit, ce qui peut contribuer à un meilleur contrôle des matrices de flux des équipements de filtrage réseau ;
- les serveurs intermédiaires peuvent apporter des fonctionnalités additionnelles dans la transmission des journaux (comme la compression ou le chiffrement), ce qui est particulièrement utile si des liens de faible capacité ou non sûrs sont utilisés pour véhiculer les journaux jusqu'aux serveurs centraux. Il est recommandé de redonder également les serveurs de collecte intermédiaires.

Document B8 : Configurer le protocole Syslog sur un équipement Cisco

Pour implémenter une configuration Syslog sur un équipement Cisco :

- Activation et paramétrage du nom du serveur Syslog auquel envoyer les messages Syslog

  #config logging syslog host *server_name*

- Supprimer un serveur syslog

  #config logging syslog host *server_name* delete

- Configurer le niveau de gravité maximum pour le filtrage des messages Syslog

  #config logging syslog level *severity_level*

- Filtrer des messages selon la catégorie

  #config logging syslog facility *facility-code*

  Exemple :

  #config logging syslog facility kern,user

Document B9 : Fonctions de filtrage Syslog

Fonctions de filtrage	Description du nom
facility()	Filtre les messages en fonction de la catégorie.
filter()	Appelle une autre fonction de filtre.
fromhost ()	Filtre les messages en fonction de l'émetteur relais.
hostname()	Filtre les messages en fonction de l'hôte émetteur.
inlist()	Filtre selon une liste blanche et/ou une liste noire.
level() ou priority()	Filtre les messages en fonction de leur priorité.
match()	Utilise une expression régulière pour filtrer les messages en fonction d'un en-tête ou d'un champ de contenu spécifié.
message()	Utilise une expression régulière pour filtrer les messages en fonction de leur contenu.
program()	Filtre les messages en fonction de l'application émettrice.
tags()	Sélectionne les messages ayant la balise spécifiée.

Document B10 : Principes de sauvegarde

Principe de la règle 3-2-1 :

- 3 - Utiliser au minimum 3 copies.
- 2 - Utiliser 2 types de supports différents.
- 1 - Avoir une copie hors site.

Le stockage à trois copies minimise considérablement le risque de perte de données. Supposons que l'on sauvegarde les données d'origine sur le disque n°1 et la sauvegarde sur le disque n°2. La probabilité de défaillance d'un disque est de 1/100 par an, la probabilité de défaillance simultanée des deux disques sera donc de 1/100 * 1/100 = 1/10 000.

Principe de la règle 3-2-1-1-0 :

- 3 - Conserver au moins 3 copies des données.
- 2 - Stocker les sauvegardes sur 2 supports différents.
- 1 - Stocker au moins une des copies dans un lieu hors site.
- 1 - Stocker au moins une des copies hors ligne.
- 0 - S'assurer d'avoir des sauvegardes vérifiées sans erreur.