REPUBLIQUE TOGOLAISE

Travail – Liberté – Patrie

UNIVERSITE DE LOME

Université de Lomé

RAPPORT DE CERTIFICATION DU RESEAU INTRANET DE L'UNIVERSITE DE LOME

COMMANDE N°00011/2024/DC/UL/S/BA

BUY MORE

ADRESSE

BUYMORE SARL U – 22 Avenue des Evala

TELEPHONE

+228 90 97 76 05 / 96 07 38 32 / 22 50 02 08

BP

22 BP 177 Lomé-Togo

EMAIL

info@buymoretogo.com / stbuymore@yahoo.fr

SITE WEB

www.buymoretogo.com

TABLE DE MATIERE

PE

I. RESUME EXECUTIF

a. Objectif de l'audit

La certification du réseau intranet de l'Université de Lomé s'inscrit dans le cadre d'un audit de validation, dont l'objectif principal est d'évaluer la mise en œuvre des recommandations issues de l'audit initial du Système d'Information (SI). Il vise à :

- vérifier l'état d'avancement des actions correctives et des améliorations apportées ;
- identifier les éventuelles lacunes persistantes ou nouvelles vulnérabilités ;
- s'assurer de la conformité du SI aux bonnes pratiques et standards de sécurité ;
- proposer des recommandations stratégiques pour renforcer la résilience et la gouvernance du SI.

b. Contexte de l'audit initial

L'audit initial du SI de l'Université de Lomé a mis en lumière plusieurs failles de sécurité et insuffisances impactant la confidentialité, l'intégrité et la disponibilité des systèmes.

Parmi les principales observations :

- absence de gouvernance IT et de documentation du SI ;
- manque de contrôle des accès physiques et logiques aux ressources critiques ;
- absence de solution de centralisation des logs et d'outils de supervision avancés ;
- vulnérabilités sur l'infrastructure réseau et les systèmes applicatifs ;
- absence d'une politique de gestion des mises à jour et des vulnérabilités ;
- faiblesse des mesures de sauvegarde et de continuité d'activité ;
- absence de segmentation du réseau.

Face à ces constats, des recommandations stratégiques ont été formulées pour renforcer la sécurité et l'efficacité du SI de l'université.

c. Méthodologie utilisée

L'audit de validation a été conduit selon une approche multicritère et structurée, combinant :

- analyse documentaire : rapport de l'audit initial et architecture réseau à jour ;
- tests techniques : scans de vulnérabilités ;
- entretiens avec les parties prenantes : DSI et équipes IT ;
- revue des mesures de sécurisation mises en place depuis l'audit initial ;
- benchmark avec les bonnes pratiques et standards internationaux.

PB

II. PRINCIPAUX RÉSULTATS

a. Avancées Significatives

L'audit de validation a permis d'identifier des progrès notables :

- Installation d'un système de vidéosurveillance dans les salles serveurs ;
- Correction de vulnérabilités critiques identifiées lors de l'audit initial ;
- Segmentation du réseau pour une meilleure gestion des flux ;
- Intégration d'un antivirus en mode client pour renforcer la sécurité des postes de travail ;
- Mise en place d'une solution de détection des vulnérabilités ;
- Intégration de Nagios pour la surveillance du réseau ;
- Renforcement des compétences des administrateurs via des formations continues ;
- Optimisation du refroidissement des salles serveurs par installation de nouveaux climatiseurs ;
- Installation d'onduleurs et de groupes électrogènes pour assurer la continuité de l'alimentation électrique ;
- Reprise des câblages non conformes des sites distants ;
- Mise en place d'une infrastructure réseau normalisée (liaisons en fibre optique, suppression des équipements non conformes comme les switchs NETIS) ;
- Renforcement de la gestion des accès (restrictions sur les locaux informatiques, filtrage des ports inutiles) ;
- Adoption de protocoles sécurisés (SSH, SFTP, HTTPS) et désactivation des versions obsolètes de SSL/TLS ;
- Mise à jour des applications critiques (PHP, JQuery) ;
- Centralisation des connexions Internet via la DRSI.

PE

b. Points en Cours de Traitement

L'Université est actuellement en phase de mise en œuvre des actions suivantes :

- Raccordement des 34 bâtiments au cœur du réseau ;
- Acquisition d'équipements homogènes ;
- Remplacement du switch de la DRSI par un cluster de niveau 3 ;
- Mise en place d'un contrôle dynamique des accès à Internet selon les périodes d'affluence ;
- Installation des équipements de distribution dans des racks normalisés ;
- Renforcement de la politique de sécurité en imposant des protocoles chiffrés (SSH, SFTP, HTTPS) ;
- Migration vers des systèmes d'exploitation pris en charge (Windows Server 2016/2019, Windows 10,11) ;
- Désactivation du stockage des identifiants Windows via le LM Hash ;
- Restriction des droits d'installation aux administrateurs systèmes ;
- Rédaction du Schéma Directeur ;
- Remplacement progressif des câbles réseau de mauvaise qualité.

c. Actions non encore démarrées

Certaines actions critiques restent à initier et nécessitent une attention particulière :

- Déploiement d'une solution antivirus unifiée sur tout le parc informatique ;
- Restriction stricte des droits d'installation aux seuls administrateurs systèmes ;
- Blocage de l'utilisation des supports amovibles pour tous les utilisateurs ;
- Mise en place d'un pare-feu LAN pour la gestion du trafic interne ;
- Application de politiques GPO pour le verrouillage automatique des sessions utilisateurs.

III. Nouvelles recommandations pour l'optimisation et la sécurisation du réseau

À la suite de ce nouvel audit de certification, de nouvelles recommandations sont formulées à l'attention de la DRSI afin d'optimiser la performance du réseau, tant en termes de gestion que de sécurisation. Ces recommandations non exhaustives sont les suivantes :

PE

a. Refonte de l'infrastructure réseau

Un datacenter normé est essentiel pour garantir la sécurité, la disponibilité et la performance des infrastructures informatiques. En respectant les normes en vigueur, il assure une meilleure résilience face aux pannes, cyberattaques et catastrophes naturelles.

Ainsi, en complément des recommandations de l'audit initial sur la nouvelle architecture cible, nous proposons la construction de deux nouveaux datacenters, l'un situé au nord et l'autre au sud de l'Université de Lomé, afin de pallier les insuffisances des infrastructures actuelles jugées inadaptées.

- Le premier datacenter servira de site primaire, hébergeant les ressources critiques.
- Le second sera une réplique du primaire, garantissant la redondance et la continuité des services en cas de défaillance du premier.

L'infrastructure réseau de l'Université s'appuiera sur ces deux salles, qui seront interconnectées et renforcées par un bouclage au niveau Edge (Zone Internet) et Cœur (Zone centrale du réseau).

b. Sécurité des applications WEB

Afin de renforcer la sécurité des applications web de l'Université de Lomé, nous recommandons vivement la mise en place d'un Web Application Firewall (WAF). Ce dispositif de sécurité permettra de filtrer et de surveiller les requêtes HTTP/HTTPS entrant et sortant des serveurs web, afin de protéger ces derniers contre diverses attaques telles que l'injection SQL, les cross-site scripting (XSS), les attaques par force brute, et d'autres menaces en rapport avec les applications web.

c. Sécurité du serveur de messagerie

Pour renforcer la protection du serveur de messagerie de l'Université de Lomé contre les attaques sophistiquées ciblant les emails tels que : phishing, malware, usurpation d'identité ; nous recommandons la mise en place d'un ProxyMail.

d. Solution EDR pour une protection Avancée

Face à l'évolution des cybermenaces de plus en plus sophistiquées, il est essentiel pour l'Université de Lomé d'adopter une approche proactive et moderne en matière de cybersécurité.

Traditionnellement, les solutions antivirus reposent sur une détection basée sur des signatures : elles comparent les fichiers et applications à une base de données de logiciels malveillants connus, puis prennent des mesures correctives (quarantaine ou suppression). Cependant, cette approche est limitée face aux nouvelles menaces Zero-Day, aux ransomwares évolutifs et aux attaques ciblées.

PE

Ainsi, nous recommandons l'implémentation d'une solution de type EDR (Endpoint Detection and Response).

e. Solution de centralisation et de corrélation des logs (SIEM)

Actuellement, l'Université de Lomé ne dispose pas d'une solution de gestion centralisée des logs, ce qui rend difficile la surveillance continue de son infrastructure informatique. Les incidents de sécurité peuvent passer inaperçus, augmentant ainsi les risques liés aux cyberattaques. La centralisation et la corrélation des logs sont essentielles pour garantir une visibilité complète et une détection rapide des anomalies ou des événements de sécurité.

Pour renforcer la sécurité du Système d'Information (SI) de l'Université, nous recommandons la mise en place d'un SIEM (Security Information and Event Management) pour centraliser et corréler les logs provenant des différents dispositifs, applications et services au sein de l'infrastructure.

f. Mise en place d'une équipe SOC dédiée ou externalisée

L'Université de Lomé, tout comme de nombreuses autres institutions, fait face à une évolution rapide des menaces informatiques. La cybercriminalité devient de plus en plus sophistiquée, et la gestion proactive de la sécurité devient primordiale. Cependant, avec la complexité croissante des cybermenaces, une simple gestion réactive des incidents ne suffit plus. Il est essentiel d'avoir une équipe spécialisée capable de surveiller, détecter et répondre rapidement à toute tentative d'intrusion ou incident de sécurité.

Ainsi, nous recommandons la mise en place d'une équipe SOC (Security Operations Center), soit internes à l'Université de Lomé ou externalisées par le biais d'un fournisseur de services spécialisés, afin de renforcer la capacité de l'université à gérer la cybersécurité de manière proactive.

g. Mise en place de tests d'intrusion réguliers

Les tests d'intrusion (ou **pentests**) sont une composante clé de toute stratégie de cybersécurité efficace. Ils permettent de simuler des attaques réelles sur le système d'information afin de détecter des vulnérabilités, d'évaluer la résistance du système aux attaques externes et internes et de mettre en évidence les faiblesses dans les mécanismes de défense en place.

Nous recommandons la mise en place de tests d'intrusion réguliers, effectués par des experts en sécurité, pour identifier les vulnérabilités critiques, valider l'efficacité des contrôles de sécurité en place et garantir que les mesures de protection et de détection des menaces fonctionnent correctement

PE

h. Mise en place d'une plateforme de sensibilisation des utilisateurs

L'un des maillons les plus vulnérables d'un système d'information est l'utilisateur final. Les cyberattaques modernes exploitent souvent des failles humaines via l'ingénierie sociale, les phishing, l'utilisation de mots de passe faibles, ou encore le manque de vigilance face aux menaces numériques.

À l'Université de Lomé, il est donc crucial de renforcer la culture de cybersécurité auprès des enseignants, du personnel administratif et dans la mesure du possible des étudiants à travers une plateforme de sensibilisation et de formation continue.

Nous recommandons la mise en place d'une plateforme dédiée qui servira à :

- Former et sensibiliser les utilisateurs aux bonnes pratiques en matière de cybersécurité
- Tester et évaluer régulièrement leur niveau de connaissance à travers des simulations et des exercices pratiques
- Diffuser des alertes de sécurité en cas de menaces ou d'attaques détectées
- Donner accès à des ressources pédagogiques (vidéos, articles, webinaires, guides interactifs)

i. Mise en place d'une solution Helpdesk

Dans le but d'améliorer la gestion des incidents à l'université de Lomé, nous recommandons la mise en place d'une solution Helpdesk centralisée et performante

CONCLUSION

L'audit de certification a permis de constater des avancées majeures dans la sécurisation du SI de l'Université de Lomé, bien que des axes d'amélioration subsistent. La mise en œuvre des actions en cours et l'initiation des mesures non encore démarrées sont essentielles pour atteindre une conformité optimale aux standards de sécurité et de gouvernance IT. Un suivi rigoureux est recommandé pour garantir la réussite de cette transformation.

SIGNATURES :

POSIA Essohouna

KPELI Komivi Rodrigue

Responsable Technique

Directeur General